ADMINISTRATOR'S GUIDE

KASPERSKY HOSTED SECURITY SERVICES

Dear User!

Thank you for choosing our product. We hope that this documentation will help you in your work and will provide answers regarding this software product.

Warning! This document is a property of Kaspersky Lab Ltd, and all rights to this document are reserved by the copyright laws of the Russian Federation and international treaties. Illegal reproduction and distribution of this document or parts hereof result in civil, administrative or criminal liability pursuant to the laws of the Russian Federation.

All materials may only be duplicated, regardless of form, or distributed, including in translation, with the written permission of Kaspersky Lab.

This document, and graphic images related to it, can be used exclusively for information, non-commercial or personal purposes.

This document may be amended without prior notification. For the latest version of this document refer to Kaspersky Lab's website at http://www.kaspersky.com/doc.

Kaspersky Lab shall not be liable for the contents, quality, frequency of updates, or accuracy of materials used in this document that belong to other individuals or entities, including liability for any potential losses associated with use of these materials.

This document includes registered and non-registered trademarks. All trademarks remain the property of their corresponding owners.

© Kaspersky Lab, 1997-2009. All rights reserved

Revision date: 28.04.2009

CONTENTS

INTRODUCTION 7
Navigation 7
Logging in 8
Dashboard Page 9
WEB VIRUS SERVICE 11
Web Virus Summary Page 11
To view summary data 12
Web Virus Reports 12
Web Virus Summary Reports 12
Viewing the reports 12
Web Virus Scheduled Reports 13
Edit an existing Web Virus Scheduled Report 13
Delete an existing Web Virus Scheduled Report 14
Add a Web Virus Scheduled Report 14
Web Virus Forensic Audit 16
Viewing a Virus Event Export (Web Virus Audit) 16
User Selection Tool 17
Web Virus Notifications 19
Web Virus User Messages 19
Using variables to customize block page text 20
Web Virus Email Alerts 20
SPYWARE 22
Spyware Summary Page 22
To view summary data 23
Spyware Reports 23
Spyware Summary Reports 23
Viewing the reports 24
Spyware Scheduled Reports 24
Edit an existing Spyware Scheduled Report 25
Delete an existing Spyware Scheduled Report 25
Add a Spyware Scheduled Report 25
Spyware Forensic Audit 28
Viewing a Virus Event Export (Spyware Audit) 28
Spyware Management 29
Adware programs 29
Spyware Notifications 30
Spyware User Messages 30
Using variables to customize block page text 31
Spyware Email Alerts 31
FILTERING 33
Filtering Dashboard 33
Filtering Reports 35
Filtering Summary Reports 35
Viewing the reports 37

Filtering Scheduled Reports 37
Delete an existing Web Filtering Scheduled Report 38
Add a Web Filtering Scheduled Report 38
Filtering Forensic Audit 41
Allowed Traffic 41
Blocked Traffic 42
Filtering Management 43
Filters 44
Creating a new Filter 44
Editing or viewing a Filter 45
Categories. Configuring the Web Categories you would like selected 45
Domains/URLs. Configuring the Domain/URLs list 46
Content Types. Configuring the Content Types you would like to filter 47
File Types. Configuring the File Types you would like to filter 47
Deleting a Filter 48
Schedules 48
How Kaspersky Hosted Security processes Schedules 49
Creating a Schedule 49
Editing a Schedule 50
Deleting a Schedule 51
Policy 51
Adding or editing a Policy Rule 51
Ordering the Rules 54
Active/Inactive Rules 54
Deleting a Rule 55
Creating Global White and Black Lists 55
Quotas 58
Creating a Quota 58
Editing a Quota 59
Deleting a Quota 60
Global Settings 60
Separate HTTP/HTTPS Filtering 61
SearchAhead 61
Supported Search Engines 62
Steps needed to activate SearchAhead for your users 62
Changes to the search engine screens 62
Annotations 63
The SearchAhead Bubble 64
Acceptable Usage Policy Screen 65
Filtering Notifications 66
Filtering User Messages 66
Using variables to customize block page text 68
Filtering Email Alerts 68
Email generation 68
IM CONTROL 69
Configuring domains for authenticated users 69
IM Control Dashboard 69
IM Control Reports 70

IM Control Summary Reports 70
Viewing the reports 71
IM Control Scheduled Reports 71
Edit an existing IM Control Scheduled Report 71
Delete an existing IM Control Scheduled Report 72
Add an IM Control Scheduled Report 72
IM Control Forensic Audit 75
Allowed Traffic 75
Blocked Traffic 76
By Participants 77
IM Management 77
Dictionaries. Configuring the Dictionaries 78
Restrictions 78
Default Restriction 79
Creating a new Restriction 79
Editing or viewing a Restriction 79
Deleting a Restriction 79
Applications 80
Dictionaries. Configuring the Dictionaries you would like to use for Blocks/Alerts 81
Schedules 82
How Kaspersky Hosted Security processes Schedules 82
Creating a Schedule 82
Editing a Schedule 83
Deleting a Schedule 84
Policies 85
Creating a Policy 85
Editing a Policy 85
Deleting a Policy 86
IM Control Notifications 86
IM Control User Messages 87
IM Control Email Alerts 87
Email generation 88
ADMINISTRATION 89
Editing your account details 89
Group Management 89
How Kaspersky Hosted Security evaluates/prioritizes Groups 90
Creating a Directory Group 90
Editing a Directory Group Name 91
Creating a Custom Group 92
Adding or editing Usernames for a Custom Group 92
Creating a Group using IP Addresses 93
Deleting a Group 93
The Default Group 93
Duplicate Users or IP Addresses 94
Authentication Key Management 94
Connector and Authentication Key deployment scenarios 94
Case 1: Company Authentication Key and Active Directory (most popular scenario) 94
Case 2: Group Authentication Key 95

Case 3: User Authentication Key 96
Creating and deleting Authentication Keys 97
Creating an Authentication Key 97
Deactivating an Authentication Key 98
Revoking an Authentication Key 98
Mobile Setting for User Authentication Keys 99
Importing a User List 99
Email messages 100
APPENDIX: FILTERING CATEGORIES 101
KASPERSKY LAB 106

INTRODUCTION

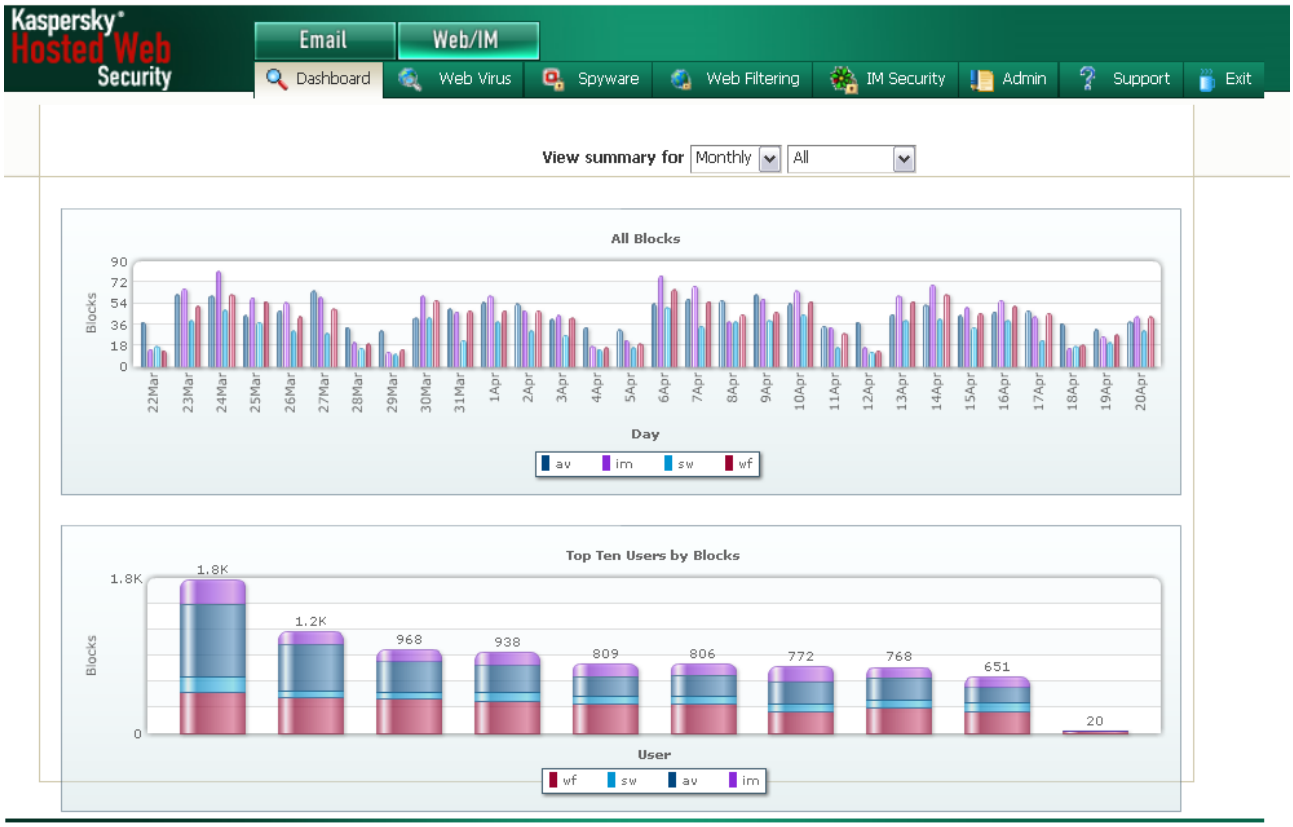
This guide explains how to set up and manage your services via the Administrator's Guide to Kaspersky Hosted Security portal.

NAVIGATION

There are seven main elements to Kaspersky Hosted Security:

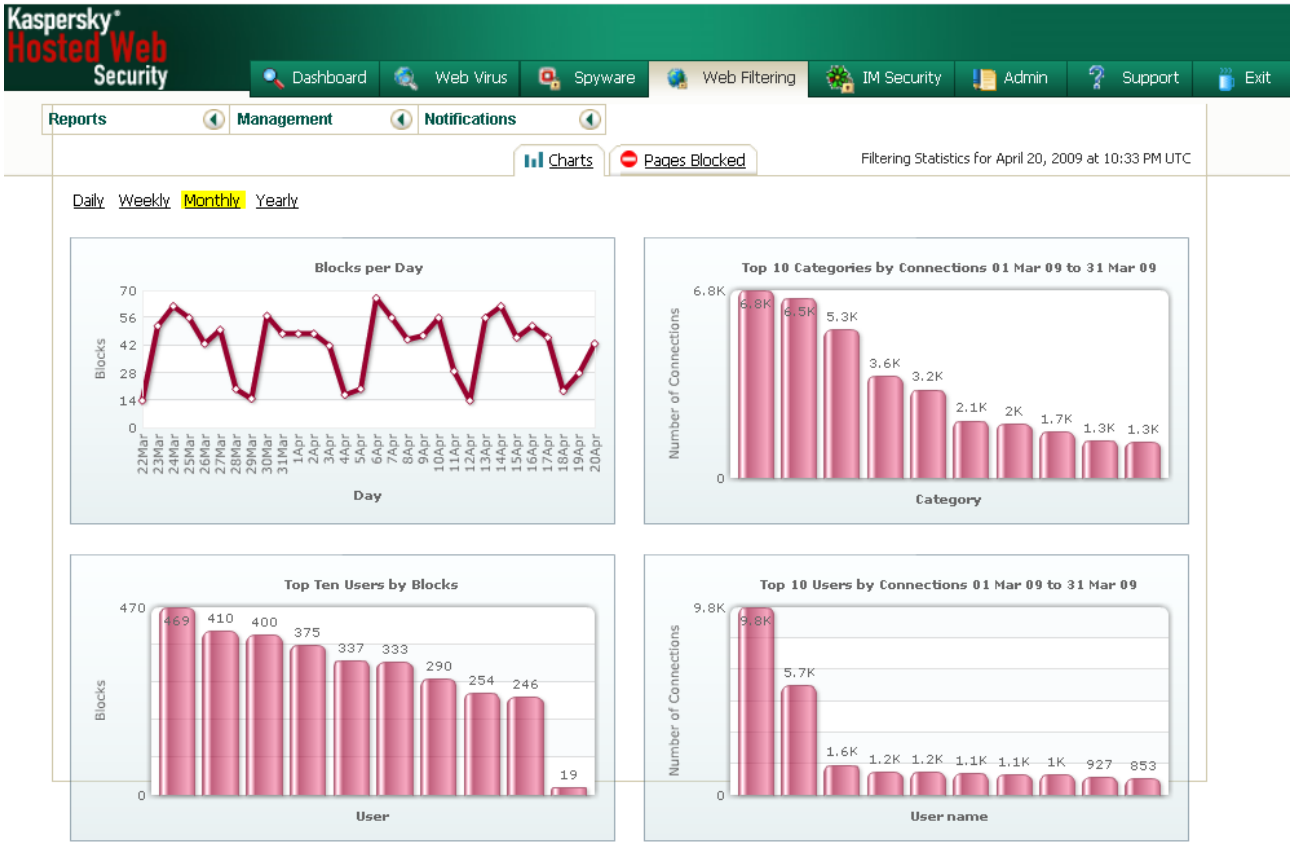
- Dashboard
- Web Virus
- Spyware
- Web Filtering
- IM Control
- Admin
- Support

These are shown as tabs at the top of the Kaspersky Hosted Security screen along with a Logout link. Simply click the tab corresponding to the function which you wish to manage.



Once you have selected a particular function, a corresponding 'sub-service' menu will appear in the left hand column. This menu includes a set of 'sub-service' buttons, which will appear for each of the four main Kaspersky Hosted Security services:

- **Reports** – provides access to a number of available reports.
- **Management** – allows you to configure and deploy usage and security policies for each of the Kaspersky Hosted Security.
- **Notifications** – allows you to set up notification settings for each service.

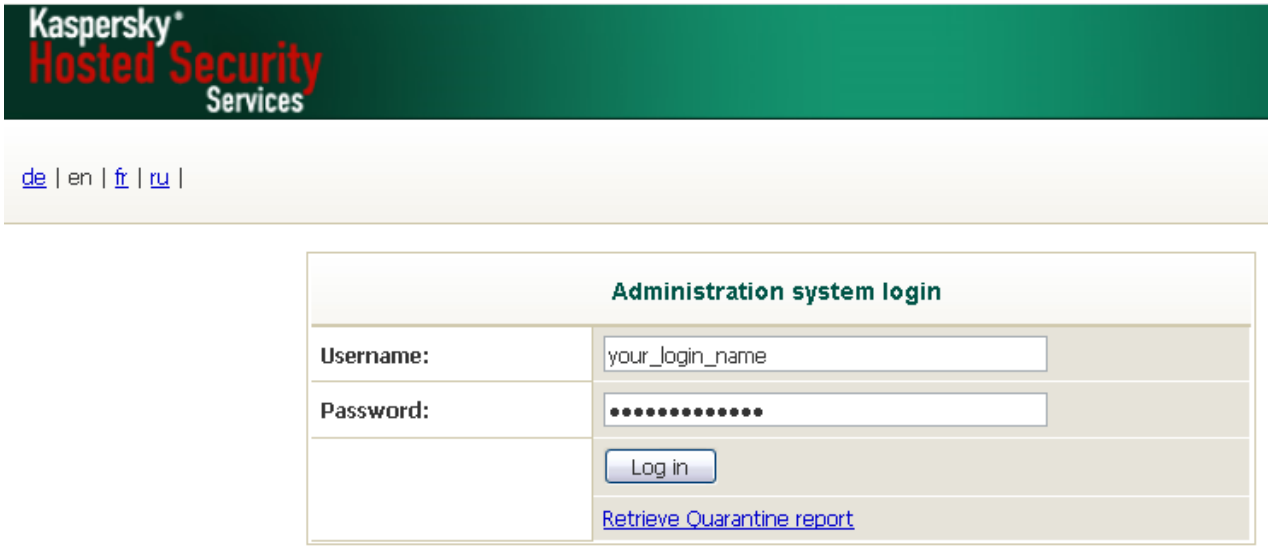


LOGGING IN

The user credentials are as specified in your initial provisioning email.

1. Enter your email address in the 'Email/Username' text field.
2. Enter your password in the 'Password' text field.
3. Click the 'Submit' button.

Both the email and password fields are case sensitive.



DASHBOARD PAGE

Once you have logged into Kaspersky Hosted Security, you will automatically be taken to the 'dashboard' page. This page welcomes you to Kaspersky Hosted Security portal and also provides you with the latest news regarding virus outbreaks, improvements to the Kaspersky Hosted Security services, and a summary of each service.

The summary for each service can be accessed through the drop down menu on the right hand side.

The table below lists the graphs that are visible in each of the drop down lists:

DROP DOWN MENU	TOP GRAPH	BOTTOM GRAPH
All	All blocks: Bar graph for all blocked events for all provisioned services for specified time period (day, week, month, year)	HTTP Hits per Day: Line graph with number of HTTP hits per day
Web Virus	**Viruses blocked:** Line chart with number of viruses detected and blocked	**Top 10 Virus blocks:** Bar chart with top 10 virus blocks and name of virus available in scroll over
Spyware	**Spyware blocks:** Line chart with number of malware instances (including spyware, adware, and phishing) detected and blocked	**Top 10 spyware blocks:** Bar chart with top 10 malware blocks and name of malware available in scroll over
Web Filtering	Web sites blocked: Line chart with number of Web sites blocked. HTTP hits per day: Line chart of number of HTTP hits per day	**Top 10 categories by connection:** Bar chart with top 10 categories and name of category available in scroll over **Top 10 Users by connections:** Bar chart with top 10 users by connections with name of user available in scroll over
IM Control	**IM blocks:** Line chart with number of IM blocks	**Top 10 IM blocks:** Bar chart with top 10 IM blocks

WEB VIRUS SERVICE

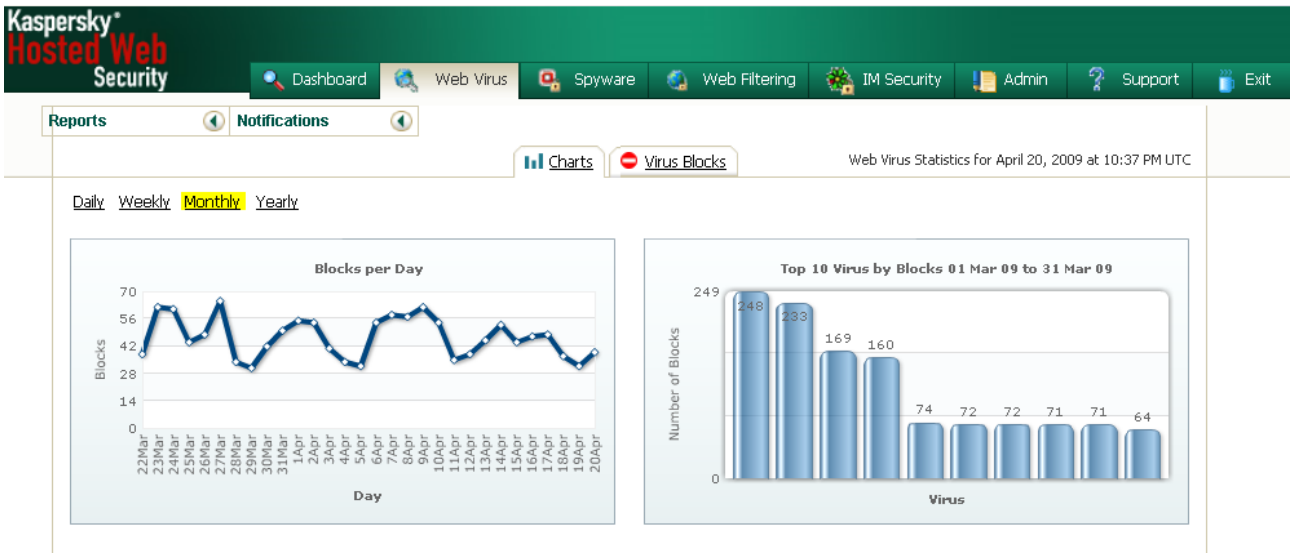
The 'Web Virus' service utilizes two sub-service buttons:

- Reports
- Notifications

Each will be described in the following sections.

WEB VIRUS SUMMARY PAGE

The Web Virus Summary sub-service lets you view related real-time Web virus activity at a glance. You can select the required time scale from the top of the window: daily, weekly, monthly, or yearly.



Web Virus Blocks: This shows the number of Web virus instances blocked by the Web Security service.

Top 10 Viruses: This shows the top viruses that have been blocked over a given time period.

Virus Blocks (table): This table displays all the malware (viruses, worms, Trojans, backdoors, etc.) blocked by the Web Security service for the given time period. The table only shows 100 entries at a time and orders them by most recent. There are links at the bottom of the table to step back in lots of 100, until you reach the very first malware blocked by the Web Security service for the given time period. For each block, the table will display:

- The date and time the malware was blocked.
- The reason it was blocked.
- The user (internal IP address) within your organization from which the request originated.
- The group the user belongs to (if available, when configured through installation of a Connector).
- The URL of the requested file.

By clicking the 'more info' button, the following information bubble will appear.

TO VIEW SUMMARY DATA

1. Click the 'Web Virus' service tab at the top of the screen. This will automatically take you to the Web Virus Reports page.

2. The default time period for the statistics displayed is for the last 24 hours (Daily). You can switch this to display weekly, monthly or yearly statistics by clicking the corresponding 'Weekly', 'Monthly' and 'Yearly' buttons located just below the main navigation bar at the top of the page.

3. You can sort the table by simply clicking the corresponding column title: Date, Reason Blocked, User, Group, and URL.

WEB VIRUS REPORTS

There are three different types of reporting available:

- Web Virus Summary Reports
- Web Virus Scheduled Reports
- Web Virus Forensic Audit.

WEB VIRUS SUMMARY REPORTS

This feature provides a Web Virus Summary Report which is available either as a table, graph or exportable file. The exportable file is provided for those who wish to import the report data into their own reporting application. This export data is available in two formats: CSV (Comma Separated Value) and XML (Extensible Mark-up Language).

The Web Security service generates this report once a day from the Internet traffic that your organization sends within a 24-hour period. The report comes in daily, weekly, monthly and yearly formats, allowing you to review all of the logged malware which your organization has blocked.

VIEWING THE REPORTS

1. Click the 'Web Virus' service tab at the top of the screen.

2. Click the 'Reports' link and select 'Summary Reports'.

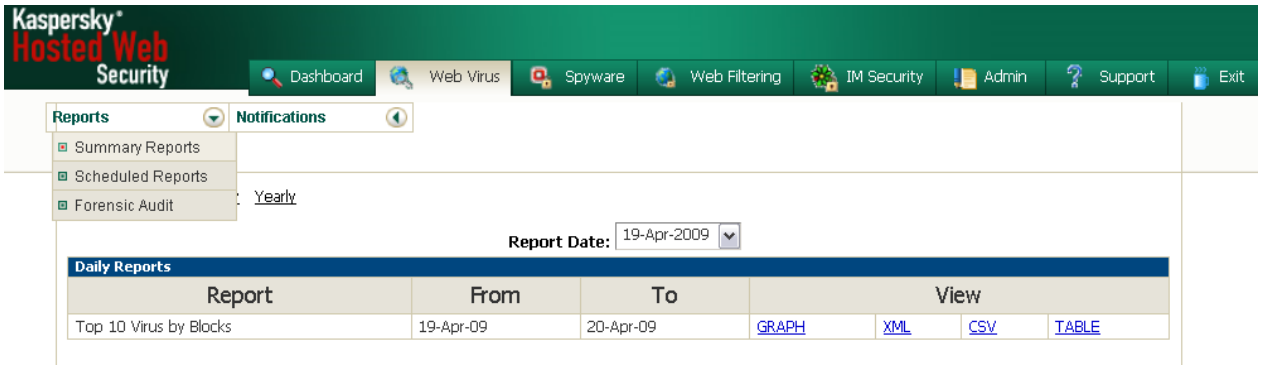
3. Select the required reporting period from the top of the page (Daily, Weekly, Monthly or Yearly).

4. From the pull-down list, select an end date for the reporting period.

5. To view a specific report, simply click the 'Graph' button located just to the right of the report's name, underneath the 'View' heading. This will open up a separate window for displaying the graph.

6. If you wish to view a report in table format, simply click the 'Table' button instead. This will open up a separate window to display the table.

7. To download the report data in either CSV or XML format, simply click the 'CSV' or 'XML' buttons. You will then be prompted by your browser to specify a save location for the data file.



WEB VIRUS SCHEDULED REPORTS

This feature provides Web Virus scheduled reporting, available either as a table, graph or both. You can select the type of presentation, report date range, users to report on, the report generation scheduled, formatting options, and who to email the report to. Kaspersky Hosted Security generates this report once a day from the Internet traffic that your organization sends within a 24-hour period.

EDIT AN EXISTING WEB VIRUS SCHEDULED REPORT

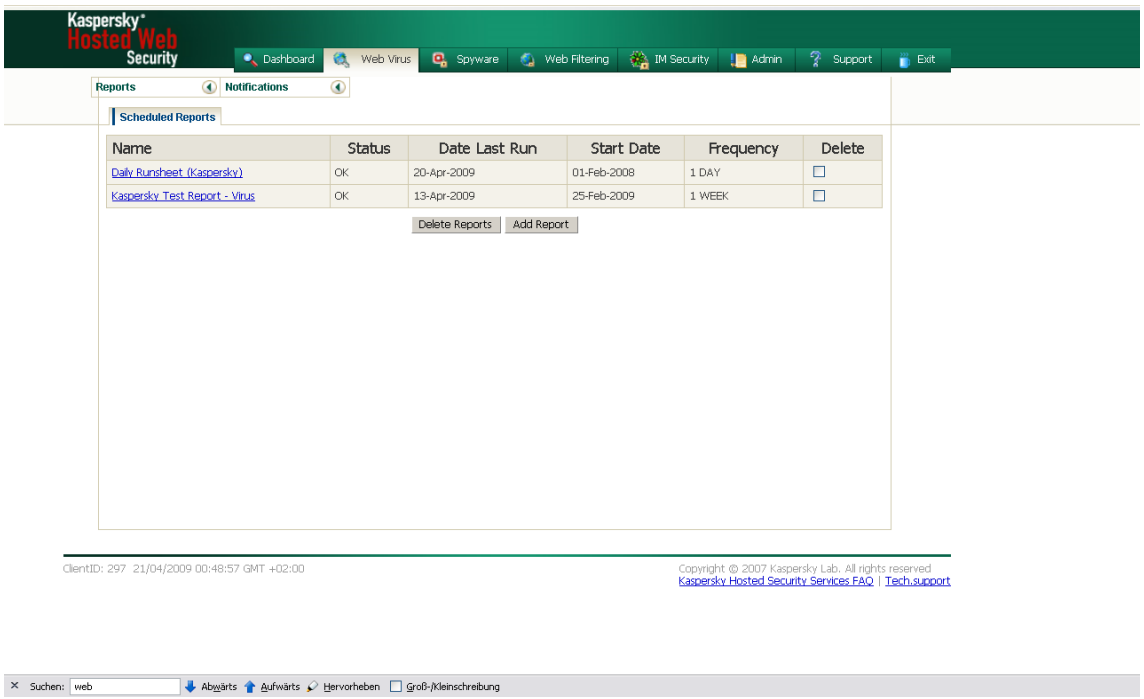
1. Click the 'Web Virus' service tab at the top of the screen.

2. Click the 'Reports' link and select 'Scheduled Reports'.

3. From the Web Virus Scheduled Reports page, you can click available reports by clicking their name, which is underlined as a link, to edit the report.

4. The report will allow you to change all options, except that the presentations that were previously selected are not editable. If you wish to change the presentations you wish to report upon, you should create a new scheduled report.

5. Once you have finished editing the existing scheduled report, click the 'Update Report' button to save your changes.

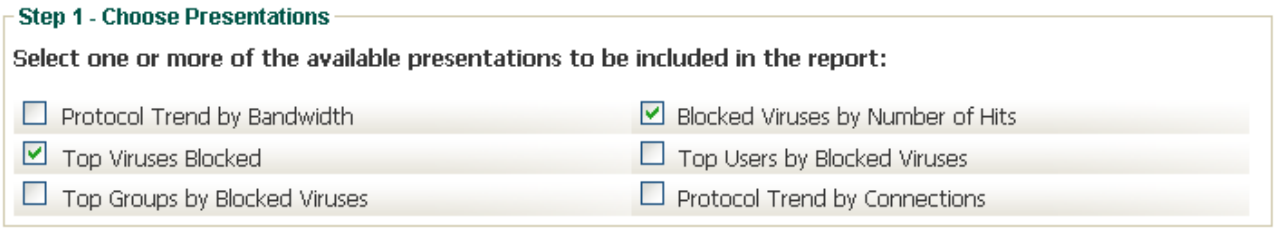


DELETE AN EXISTING WEB VIRUS SCHEDULED REPORT

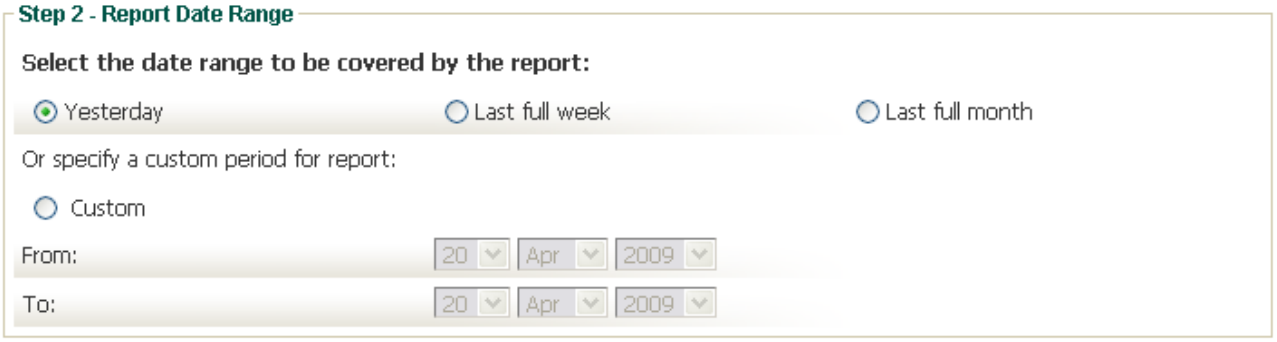
1. Click the 'Web Virus' service tab at the top of the screen.
2. Click the 'Reports' link and select 'Scheduled Reports'.
3. From the Web Virus Scheduled Reports page, you can click the checkbox to the right of the available reports, and then click the 'Delete Reports' button to delete the selected reports. A validation message will appear to ask if you are sure you want to delete the selected reports; click 'OK' to delete the reports.

ADD A WEB VIRUS SCHEDULED REPORT

1. Click the 'Web Virus' service tab at the top of the screen.
2. Click the 'Reports' link and select 'Scheduled Reports'.
3. From the Web Virus Scheduled Reports page:
    - **Step 1**: Select from the available presentations to be included in the report:
        - Top Viruses Blocked
        - Blocked Viruses by Number of Hits
        - Top Groups by Blocked Viruses
        - Protocol Trend by Bandwidth
        - Protocol Trend by Connections
        - Top Users by Blocked Viruses


Step 1 - Choose Presentations
Select one or more of the available presentations to be included in the report:
Protocol Trend by Bandwidth
Blocked Viruses by Number of Hits
Top Viruses Blocked
Top Users by Blocked Viruses
Top Groups by Blocked Viruses
Protocol Trend by Connections

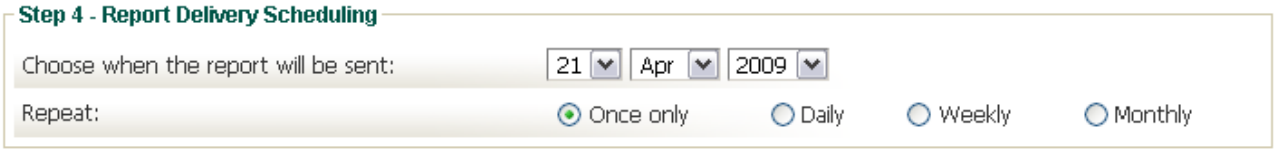
- **Step 2**: Select the desired date range required either Yesterday, Last full week, Last full month or a customized date range.



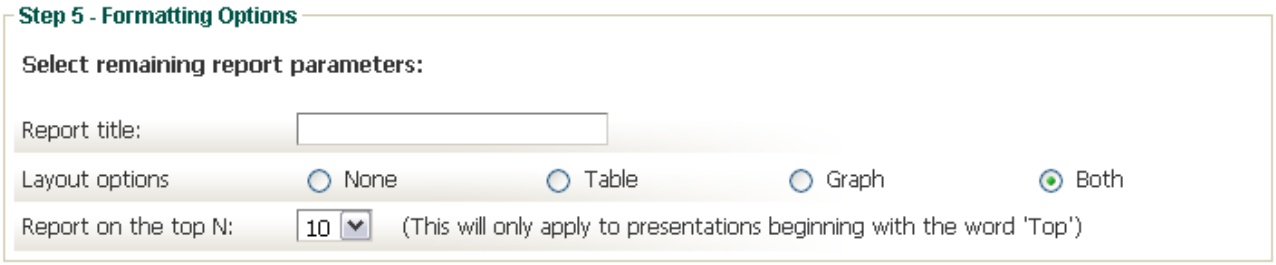
- **Step 3**: Select either all users or specific users or groups by clicking the 'Edit' button. The Groups and User IPs screen show the available groups and User or IP addresses that are available to be reported on. This data is based on the monitored traffic.

You can filter on either groups or user (not a combination of both). Clicking the Add group or Add user button will bring up a popup where you can select them, When you save, only the open filter (group or user) will be saved.

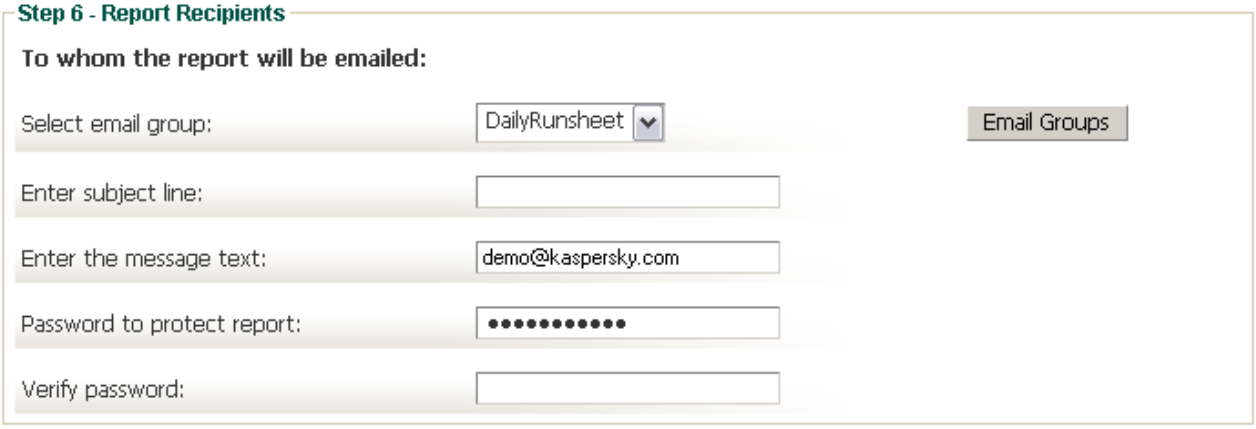
- **Step 4**: Schedule the report delivery, by selecting the specific start date using the drop down boxes, and selecting the frequency of the scheduled report delivery: either Once only, Daily, Weekly or Monthly.



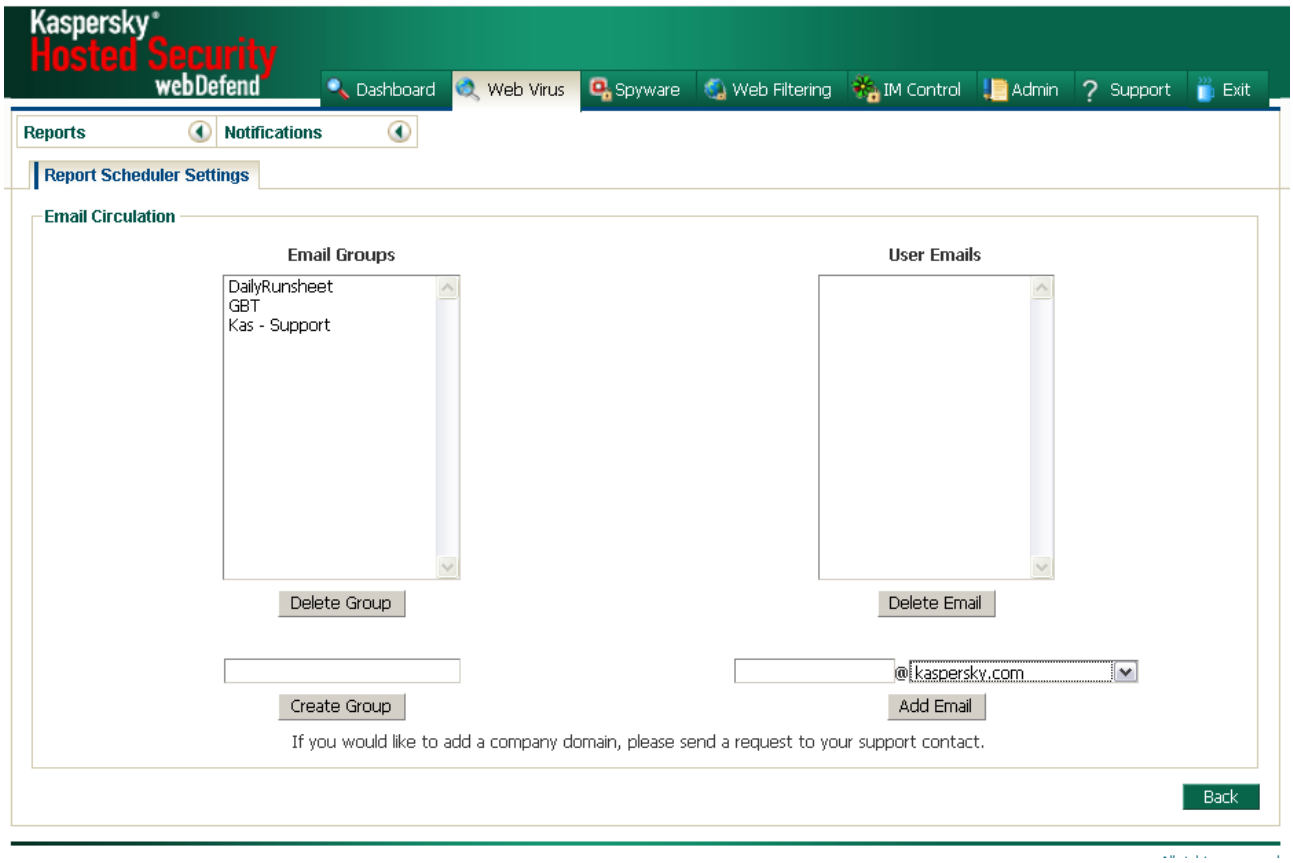
- **Step 5**: Select formatting options for the report (including typing in a report title) and layout options by selecting a table or graph presentation or both. You may also select the top 'N' (number) for the presentations you have selected, such as the 'Top 50 Viruses Blocked'.



- **Step 6**: Select the report recipients by selecting the email group, entering the subject line of the email, the message text and a password to open and review the report. If you want to create new email groups or edit existing ones, click the 'Email Groups' button.



Select the Email Group on the left side to see the email addresses assigned to that group on the right side. You can add new email groups, delete groups, and remove and add email addresses. Email addresses are restricted to the company domain that is created when your account is created. If you would like to add additional company domains, please send a request to KHSS-Support@kaspersky.com. Click the 'Back' button to return to the previous screen. Click the 'Activate Report' button when you have finished.



WEB VIRUS FORENSIC AUDIT

The Web Virus Forensic Audit sub-service lets you receive a detailed audit trail of all Web Virus scanning activity resulting in a blocked Web request.

VIEWING A VIRUS EVENT EXPORT (WEB VIRUS AUDIT)

1. Click the 'Web Virus' service tab at the top of the screen.
2. Click the 'Forensic Audit' link in the 'Reports' sub-service tab.
3. From the Web Virus Audit page, select the desired date range required: either Today, Yesterday, Last full week, Last full month or a customized date range. The date range can be up-to three months over the previous year.
4. Select who the audit is about – this can mean a specific user or all users. (See 'User Selection Tool' on page 17 for more information).
5. Click 'Generate Audit'.
6. From the pop-up, select 'Open' to immediately view the file in Excel, or select 'Save' to save the data in a CSV Excel file.

The requested activity is exported to a CSV file and contains the following data:

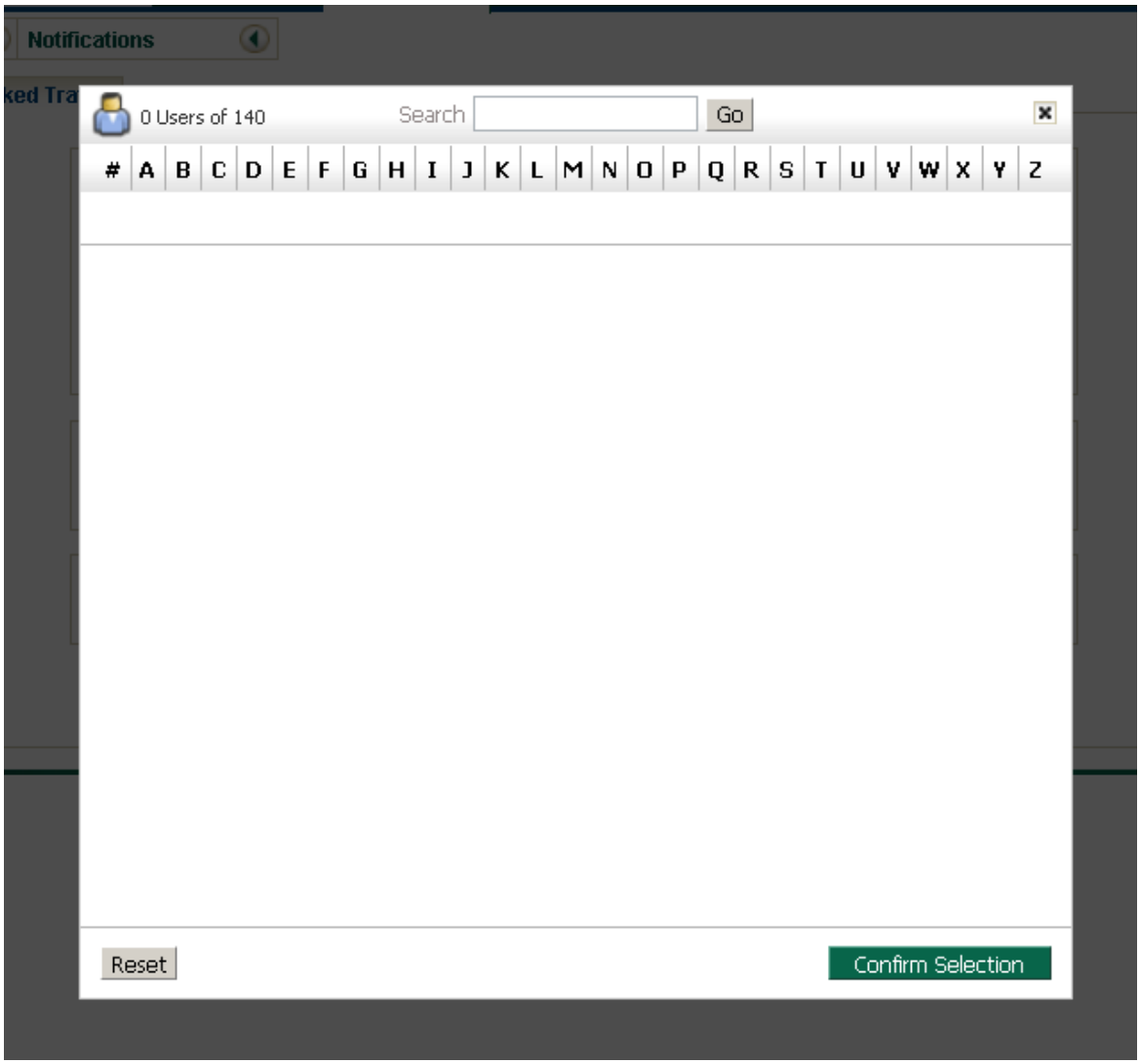
- **Date/Time** – date and time of the block.
- **Threat Type** – lists the pattern name of the offending malware (virus, worm, Trojan, etc.).
- **User** – identifies the external IP address of the customer site.
- **Internal IP** – identifies the internal IP address of the user.
- **Group** – identifies the directory group from which the Web request originated (if available – requires installation of a Connector).
- **URL** – lists the requested URL.

Date	Threat Type	User	Internal IP	Group	URL
18-Feb-2008 09:48:09 UT(	EICAR-Test-File	test@xyz.com	192.168.0.83	testgroup	http://www.eicar.org/download/eicar_com.zip
18-Feb-2008 09:48:19 UT(	EICAR-Test-File	test@xyz.com	192.168.0.83	testgroup	http://www.eicar.org/download/eicar.com
18-Feb-2008 09:48:37 UT(	oi.file.tmp.MC	test@xyz.com	192.168.0.83	testgroup	http://www.jobserve.com/WebResource.axd?d=cppv3UjMVkyHjhFr
18-Feb-2008 09:49:19 UT(	EICAR-Test-File	test@xyz.com	192.168.0.83	testgroup	http://www.eicar.org/download/eicar.com.txt
18-Feb-2008 11:42:27 UT(	oi.file.tmp.IW	WinNT://SUPPORT2003DC1\Administrato	127.0.0.1	testgroupsa	http://www.bbc.co.uk/home/images/main_promo/news/milky_w
18-Feb-2008 16:20:17 UT(	oi.file.tmp.MM	test@xyz.com	192.168.0.83	testgroup	http://www.nhs.uk/css/screen.css
18-Feb-2008 16:20:30 UT(	oi.file.tmp.MM	test@xyz.com	192.168.0.83	testgroup	http://www.nhs.uk/css/screen.css
18-Feb-2008 16:20:45 UT(	oi.file.tmp.MM	test@xyz.com	192.168.0.83	testgroup	http://www.nhs.uk/css/screen.css

USER SELECTION TOOL

When you need to specify an individual user in the forensic report, this is achieved by clicking the ‘Select user’ button,

At this point the screen will darken and a user selection tool will appear. At the top left you can see the total number of unique users in the system.



There are two ways to select an individual user: search mode or alphabet search. Please note that the system is designed to search for usernames, so those in Active Directory format (WinNT://domain\user) can only be searched for the username part of the string. The system will display the complete active directory string for those users which are registered in this way.

Search Mode

In Search Mode you can enter in a name of part of a name to the Search box and click the '**Go**' button. All of the names which have matched the search will appear in the list of names below.

Alphabet search

1. In the Alphabet search mode, you can click the letter of the alphabet which corresponds to the start of the username.

2. Once you have found the required user, click the '**Select**' button. The user will now change color and the '**Select**' button will change to '**Deselect**'.

3. Now click the '**Confirm Selection**' button to return to the previous screen with the user now active in the filter.

WEB VIRUS NOTIFICATIONS

Under the **Web Virus Notifications** sub-service tab, there are two settings which require configuration:

- **User Messages** – specifies the message which an end-user will see when a Web request is blocked.
- **Email Alerts** – lets the administrator receive an email alert when malware is blocked.

Further information is given on these settings below.

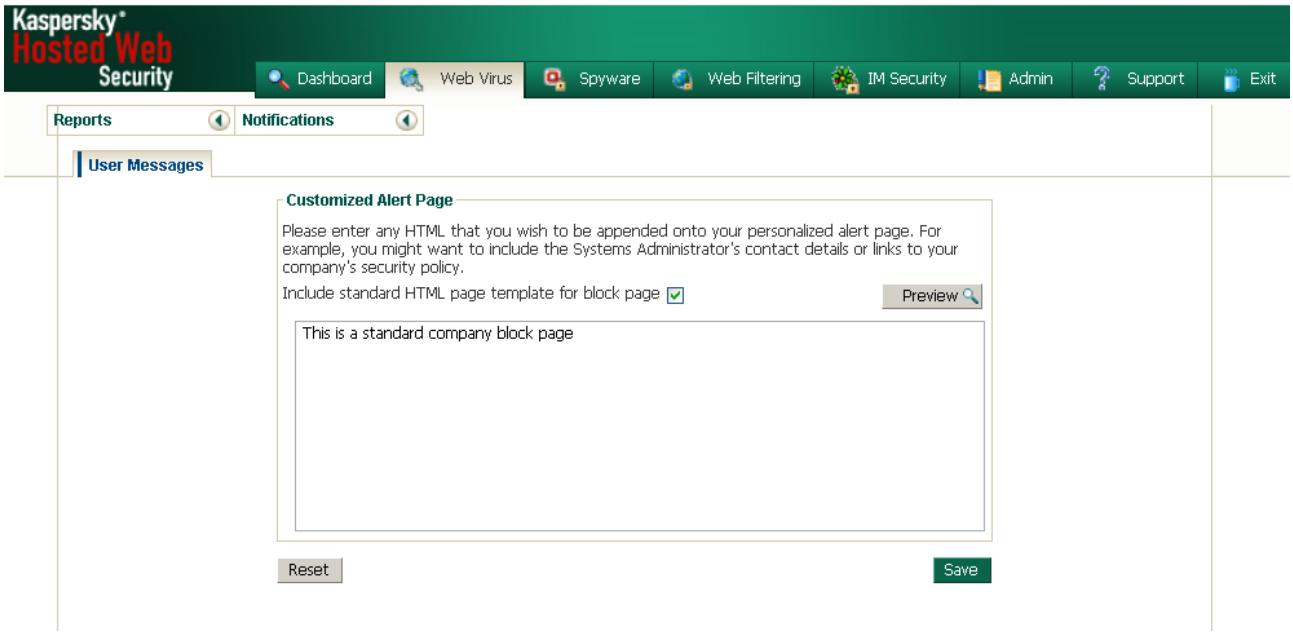
WEB VIRUS USER MESSAGES

The Web Security Service User Message is the page that your users will see in their Web browser if a URL they request is blocked. In order to customize it for your organization, you can append your own information and add your company logo to the Default Alert Page. For example, you may wish to add the Systems Administrator's contact details, or links to your organization's security policy.

The custom information must be submitted in HTML.

Kaspersky Hosted Security allows for fully customizable block pages, which means that you can define the entire HTML output of the block page up to and including the opening and closing <html> tags. This allows you to customize block pages with your own logo and text on the block page.

1. Click the 'Web Virus' service tab at the top of the screen.
2. Click the 'User Messages' link in the 'Notifications' sub-service tab. This will bring up the 'User Messages' screen.



3. Uncheck the 'Include Kaspersky Lab headers' box to remove the Kaspersky Lab logo from the block page.
4. Enter the desired HTML into the 'User Messages' field. Any images/css referenced needs to be a resolvable location. Typically you will be required to host your own images/css for this page.
5. You may insert #reason, #url, #category or #username into the HTML and it will be parsed as the reason for the block event. More detail is available in the next section.

6. Once you are happy with the Alert Page modifications you have made, click the 'Save' button located at the bottom of the screen.

7. Click the preview button just beneath the text area to see how the additional information is rendered. You must save your changes before preview displays your new settings.

USING VARIABLES TO CUSTOMIZE BLOCK PAGE TEXT

You may insert #reason, #url, #category or #username into the HTML in your custom block page and the block page will show the reason for the block event. An example below shows this more clearly:

Default block message:

```
URL contained in custom redlist default
Blocked Category : SMS / Ring Tones / Logos
EICAR-Test-File
```

Custom HTML message written by user:

```
<b>#reason<b><br>
#reason is not allowed by acme corps
```

Custom message text will appear in end-user block page:

```
<b> EICAR-Test-File<b><br>
 EICAR-Test-File is not allowed by acme corps
```

WEB VIRUS EMAIL ALERTS

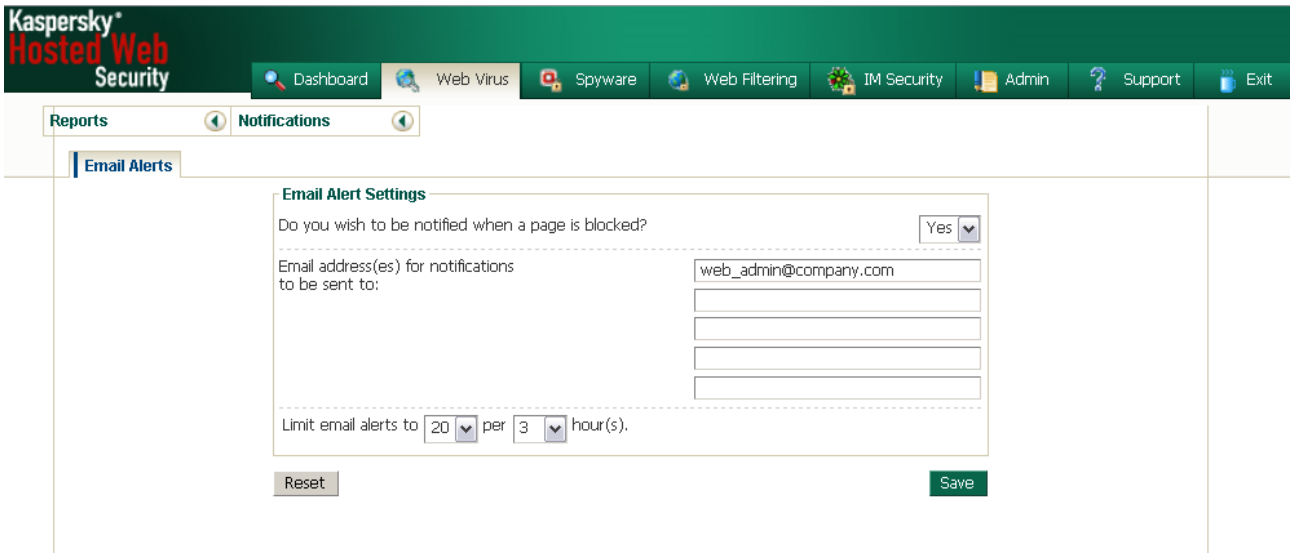
The Web Virus Email Alerts are emails that notify the administrator whenever a virus has been blocked by the Web Security Service. The email will contain the following information:

- The IP address of the Web request that left your organization.
- The reason the requested file was blocked (malware name).
- The full URL of the Web request.

To set up Web Virus Email Alerts:

1. Click the 'Web Virus' service at the top of the screen.

2. Click the 'Email Alerts' link in the 'Notifications' sub-service tab. This will bring up the 'Email Alerts' page.



3. Select whether or not you want to be notified when a virus is blocked by selecting 'Yes' or 'No' from the drop down box.

4. Enter the email address (or addresses) you want notifications to be sent to in the empty text fields provided. You can specify a maximum of five different email addresses to which you wish to have alerts sent. If you require the alerts to be sent to more addresses than this, we recommend that you set up a group mailing address.

5. If you wish to throttle the number of email alerts you receive, click in the box next to the statement 'Limit these alerts to'. Throttling will now be activated and you should select the number of alerts you wish to receive for the given number of hours you specify. For example, you might decide that you only want to receive a maximum of three email alerts in any two-hour period.

6. To save the settings and email addresses, click the 'Save' button located at the bottom of the screen.

SPYWARE

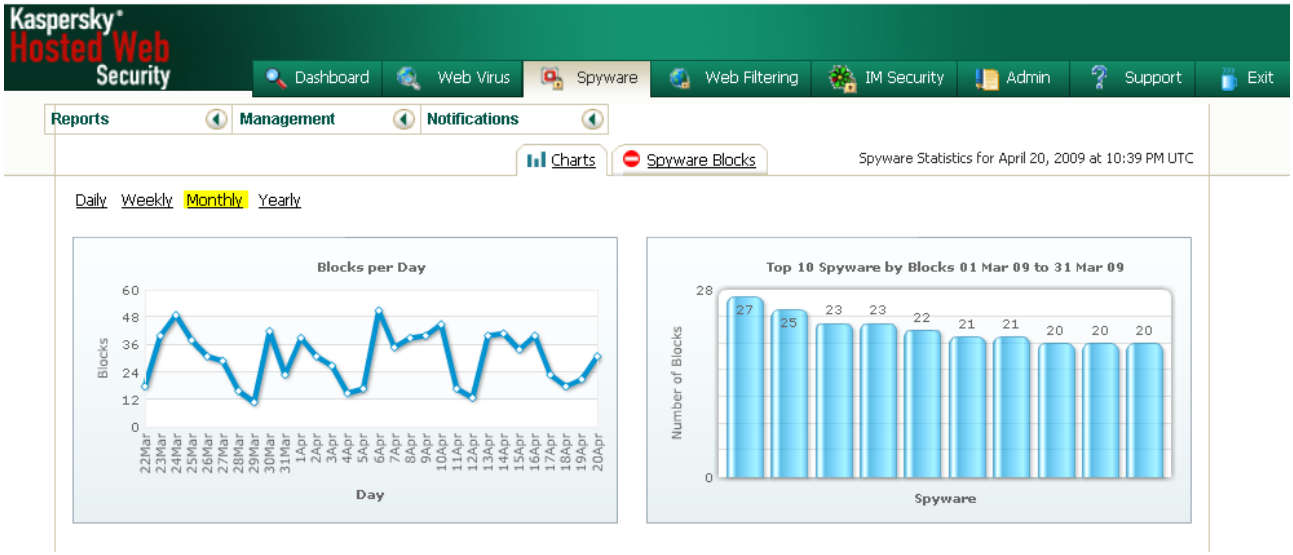
The ‘Spyware’ service utilizes three sub-service buttons:

- Reports
- Management
- Notifications

Each will be described in the following sections.

SPYWARE SUMMARY PAGE

The Spyware Summary sub-service lets you view related spyware, phishing, and adware activity at a glance. You can select the required time scale from the top of the window: daily, weekly, monthly, or yearly.



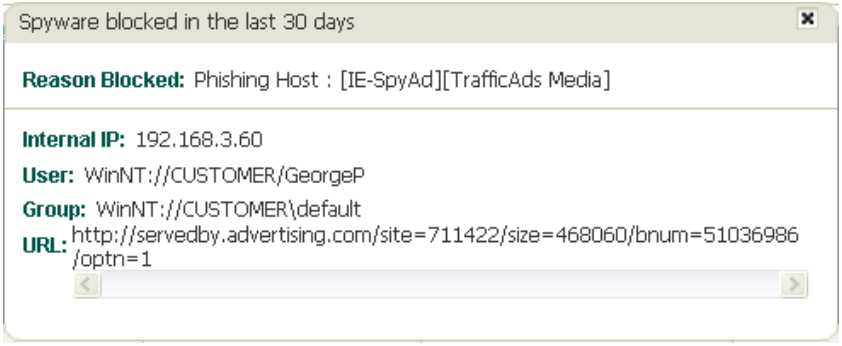
Spyware/Phishing/Adware Blocks: This shows the number of spyware, phishing and adware instances blocked by the Web Security service.

Top 10 Spyware blocks: This shows the top 10 spyware blocks over a given period of time.

Spyware/Adware/Phishing Blocks (table): This table displays all the adware programs and phishing incidents blocked by the Web Security Service for the given time period. The table shows 100 entries at a time and orders them by most recent. There are links at the bottom of the table to step back in lots of 100, until you reach the very first block by the Web Security Service for the given time period. For each malware block, the table will display:

- The date and time the malware was blocked.
- The reason it was blocked.
- The user (usually, internal IP address) within your organization from which the request originated.
- The group the user belongs to (if available, when configured through installation of a Connector).
- The URL of the requested file.

By clicking the ‘more info’ button, the following information bubble will appear.



TO VIEW SUMMARY DATA

1. Click the 'Spyware' tab at the top of the screen. This will automatically take you to the Summary Page.

2. By default, the time period for the statistics displayed on the page is for the last 24 hours. You can switch this to display weekly, monthly or yearly statistics by clicking the corresponding 'Weekly', 'Monthly' and 'Yearly' buttons located just below the main navigation bar at the top of the page.

3. You can also sort the table by simply clicking the corresponding column title: Date, Reason Blocked, User, Group, and URL.

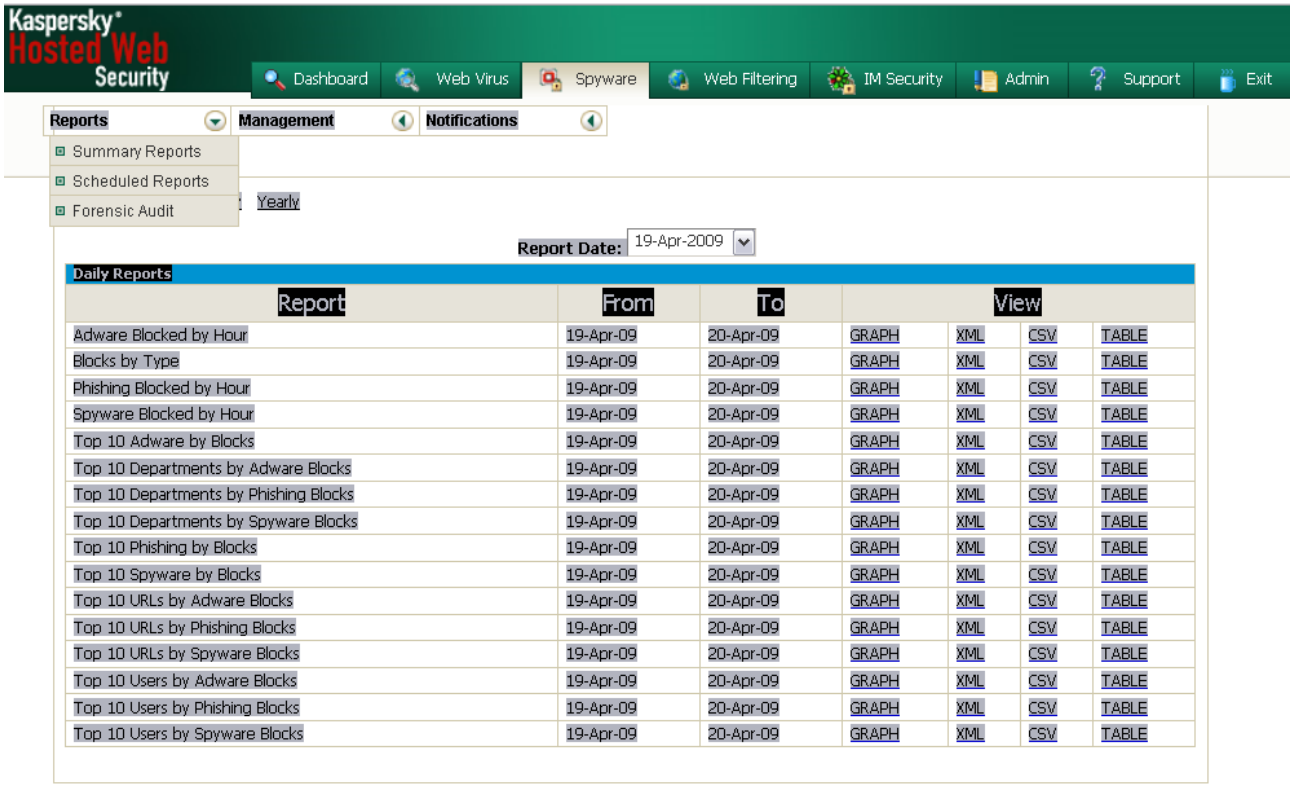
SPYWARE REPORTS

There are three different types of reporting available:

- Spyware Summary Reports
- Spyware Scheduled Reports
- Spyware Forensic Audit

SPYWARE SUMMARY REPORTS

This feature provides a Spyware Summary Report which is available either as a table, graph or exportable file. The exportable file is provided for those who wish to import the report data into their own reporting application. This export data is available in two formats: CSV (Comma Separated Value) and XML (Extensible Mark-up Language). The Web Security Service generates this report once a day from the Internet traffic that your organization sends within a 24-hour period. The report comes in daily, weekly, monthly and yearly formats, allowing you to review all of the spyware that your organization has encountered.



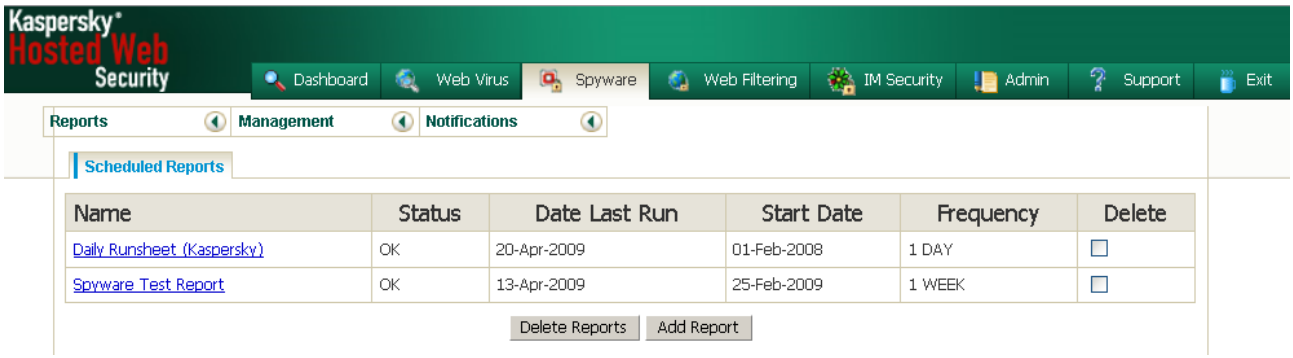
Report	From	To	View			
Adware Blocked by Hour	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Blocks by Type	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Phishing Blocked by Hour	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Spyware Blocked by Hour	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Adware by Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Departments by Adware Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Departments by Phishing Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Departments by Spyware Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Phishing by Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Spyware by Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 URLs by Adware Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 URLs by Phishing Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 URLs by Spyware Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Users by Adware Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Users by Phishing Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE
Top 10 Users by Spyware Blocks	19-Apr-09	20-Apr-09	GRAPH	XML	CSV	TABLE

VIEWING THE REPORTS

1. Click the ‘Spyware’ service tab at the top of the screen.
2. Click the ‘Reports’ link and select ‘Summary Reports’.
3. Select the required reporting period from the top of the page (Daily, Weekly, Monthly or Yearly).
4. From the pull-down list, select an end date for the reporting period.
5. To view a specific report, simply click the ‘Graph’ button located just to the right of the report’s name, underneath the ‘View’ heading. This will open up a separate window for displaying the graph.
6. If you wish to view a report in table format, simply click the ‘Table’ button instead. This will open up a separate window to display the Table.
7. To download the report data in either CSV or XML format, simply click the ‘CSV’ or ‘XML’ buttons. You will then be prompted by your browser to specify a save location for the data file.

SPYWARE SCHEDULED REPORTS

This feature provides Spyware scheduled reporting, available either as a table, graph or both. You can select the type of presentation, report date range, users to report on, the report generation scheduled, formatting options, and who to email the report to. The Spyware service generates this report once a day from the Internet traffic that your organization sends within a 24-hour period.



EDIT AN EXISTING SPYWARE SCHEDULED REPORT

1. Click the 'Spyware' service tab at the top of the screen.
2. Click the 'Reports' link and select 'Scheduled Reports'.
3. From the Spyware Scheduled Reports page, you can click available reports by clicking their name, which is underlined as a link, to edit the report.
4. The report will allow you to change all options, except that the presentations that were previously selected are not editable. If you wish to change the presentations you wish to report upon, you should create a new scheduled report.
5. Once you have finished editing the existing scheduled report, click the 'Update Report' button to save your changes.

DELETE AN EXISTING SPYWARE SCHEDULED REPORT

1. Click the 'Spyware' service tab at the top of the screen.
2. Click the 'Scheduled Reports' link in the 'Reports' sub-service tab.
3. From the Spyware Scheduled Reports page, you can click the checkbox to the right of the available reports, and then click the 'Delete Reports' button to delete the selected reports. A validation message will appear to ask if you are sure you want to delete the selected reports. Click 'OK' to delete the reports.

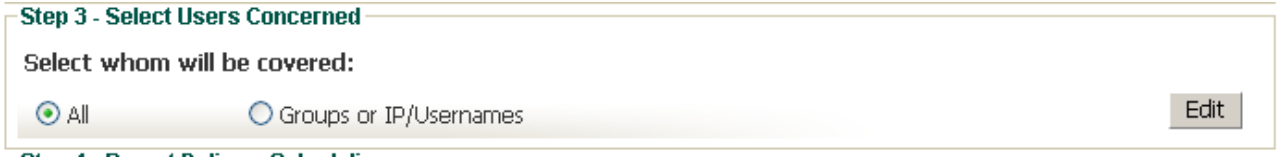
ADD A SPYWARE SCHEDULED REPORT

1. Click the 'Spyware' service tab at the top of the screen.
2. Click the 'Reports' link and select 'Scheduled Reports'.
3. From the Spyware Scheduled Reports page
    - **Step 1**: Select from the available presentations to be included in the report:
        - Top Users by Blocked Spyware
        - Top Groups by Blocked Spyware
        - Top Spyware Blocked

Step 1 - Choose Presentations
Select one or more of the available presentations to be included in the report:
Top Spyware Blocked
Top Users by Blocked Spyware
Top Groups by Blocked Spyware

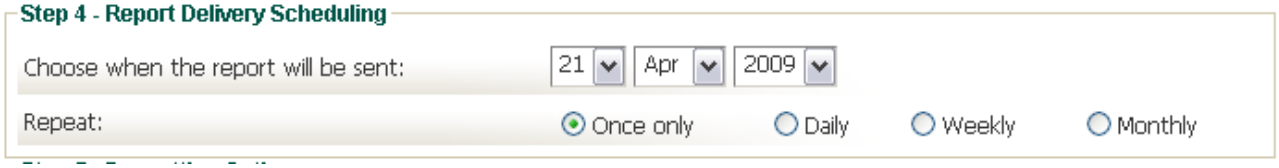
- **Step 2**: Select the desired date range required: either Yesterday, Last full week, Last full month or a customized date range.

- **Step 3**: Select either all users or specific users or groups by clicking the 'Edit' button. The Groups and User IPs screen show the available groups and User or IP addresses that are available to be reported on. This data is based on the monitored traffic.

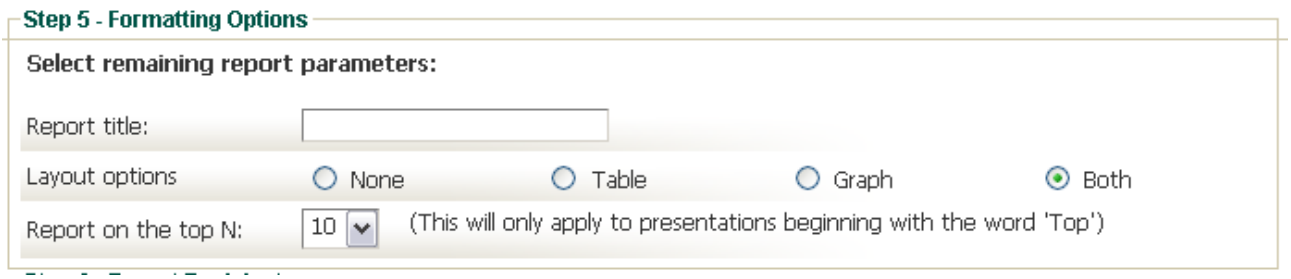


You can filter on either groups or user (not a combination of both). Clicking the Add group or Add user button will bring up a popup where you can select them, When you save, only the open filter (group or user) will be saved.

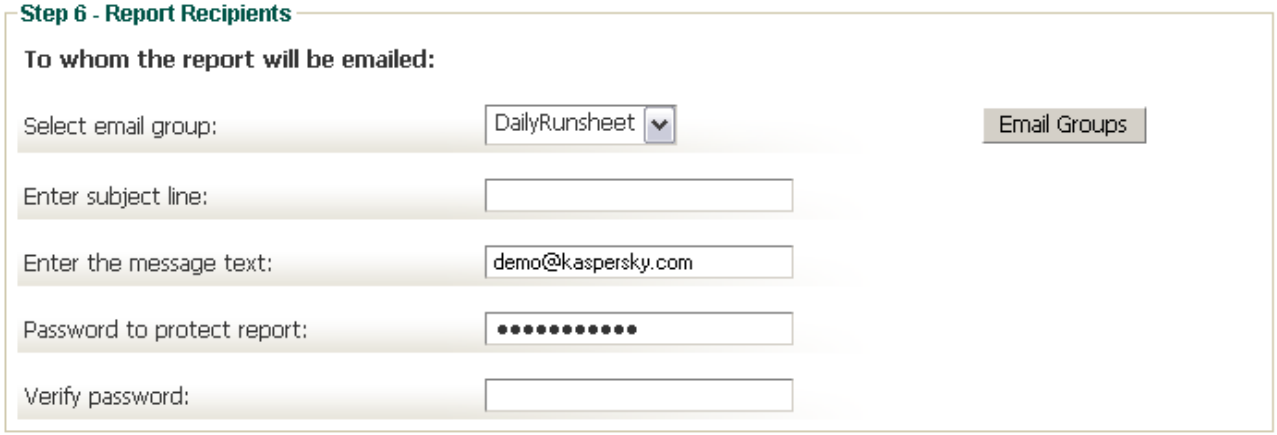
- **Step 4**: Schedule the report delivery by selecting the specific start date using the drop down boxes and selecting the frequency of the scheduled report delivery – either Once only, Daily, Weekly or Monthly.



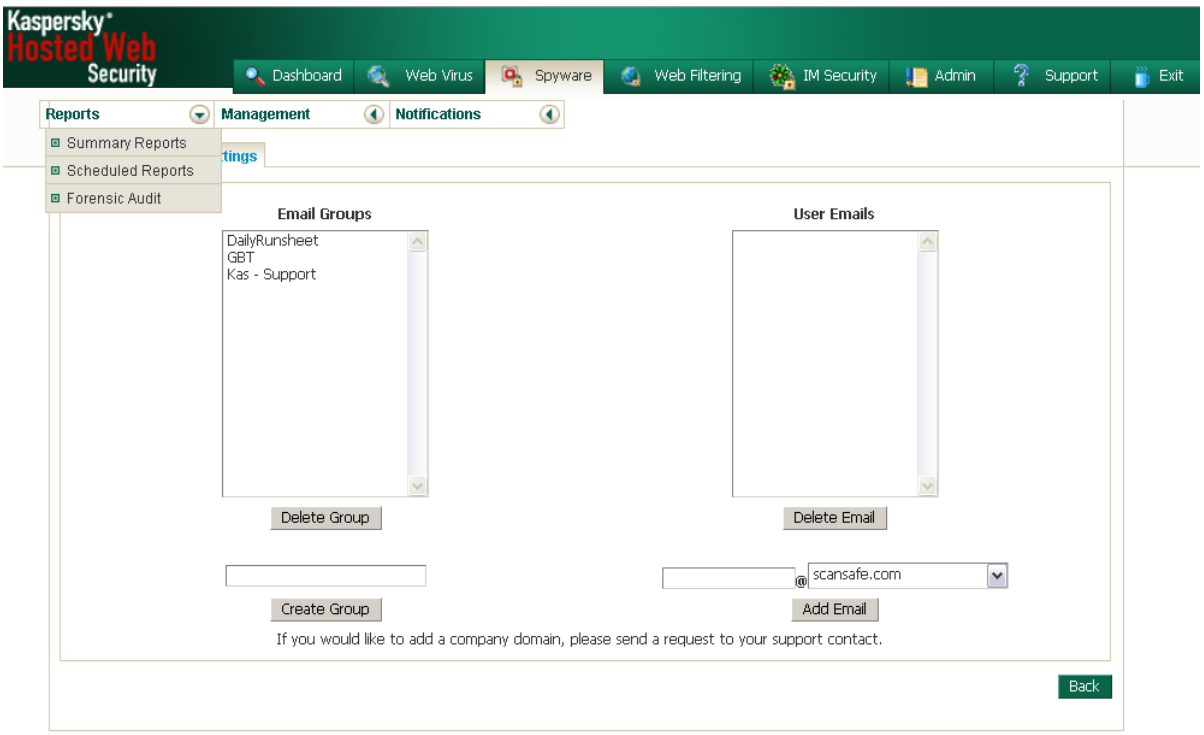
- **Step 5**: Select formatting options for the report (including typing in a report title) and layout options by selecting a table or graph presentation or both. You may also select the top 'N' (number) for the presentations you have selected, such as the 'Top 10 Users by Blocked Spyware'.



- **Step 6**: Select the report recipients by selecting the email group, entering the subject line of the email, the message text and a password to open and review the report. If you want to create new email groups or edit existing ones, click the 'Email Groups' button.



Select the Email Group on the left side to see the email addresses assigned to that group on the right side. You can add new email groups, delete groups, and remove and add email addresses. Email addresses are restricted to the company domain that is created when your account is created. If you would like to add additional company domains, please send a request to KHSS-Support@kaspersky.com. Click the 'Back' button to return to the previous screen. Click the 'Activate Report' button when you have finished.

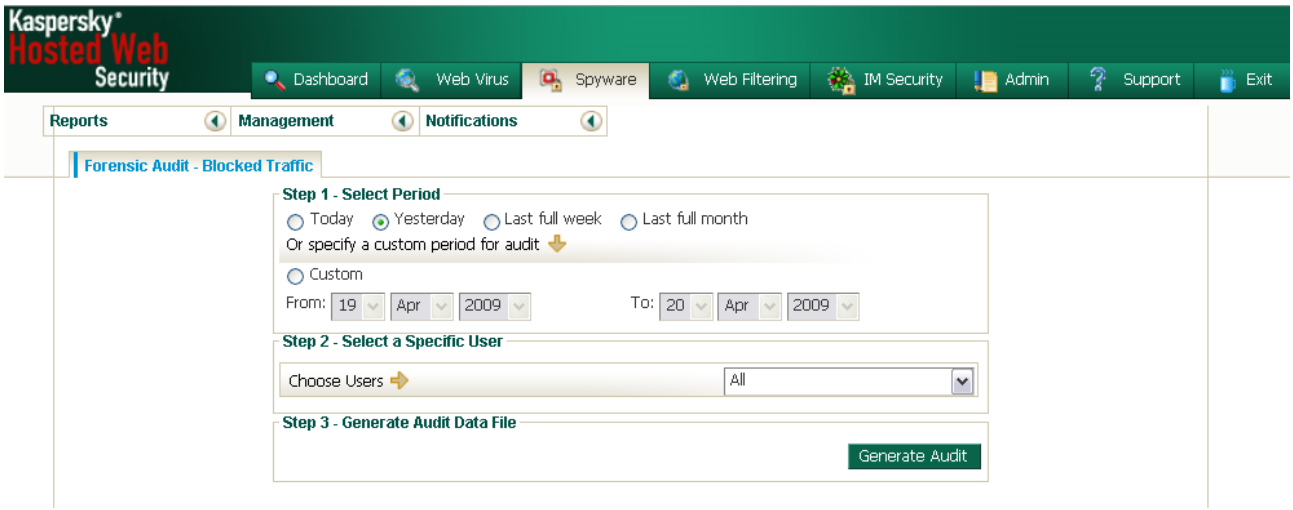


SPYWARE FORENSIC AUDIT

The Spyware Audit sub-service enables an administrator to receive a detailed audit trail of all Spyware scanning activity resulting in a blocked Web request.

VIEWING A VIRUS EVENT EXPORT (SPYWARE AUDIT)

1. Click the 'Spyware' service tab at the top of the screen.
2. Click the 'Forensic Audit' button in the 'Reports' sub-service tab.
3. From the Spyware Audit page, select the desired date range required: either Today, Yesterday, Last full week, Last full month or a customized date range. The date range can be up-to three months over the previous year.
4. Select who the audit is about – this can mean a specific user or the entire company. (See 'User Selection Tool' on page 17 for more information).
5. Click 'Generate Audit'.
6. From the pop-up, select 'Open' to immediately view the file in Excel, or select 'Save' to save the data in a CSV Excel file.



The requested activity is exported to a CSV file and contains the following data:

- **Date/Time** – date and time of the event.
- **Threat Type** – lists the pattern name of the offending malware (worm, Trojan, etc.).
- **User** – identifies the IP address of the customer site.
- **Internal IP** – identifies the internal IP address of the user.
- **Group** – identifies the directory group from which the Web request originated (if available – requires installation of a Connector).
- **URL** – lists the requested URL.

Date	Threat Type	User	Internal IP	Group	URL
18-Feb-20	Heuristic	test@xyz.com	192.168.0.83	testgroup	http://gator.com/
18-Feb-20	[Content Match]	test@xyz.com	192.168.0.83	testgroup	http://cmhtml.overture.com/
18-Feb-20	t1.extreme-dm.com	192.168.0.173	192.168.0.173	testgroupsall	http://t1.extreme-dm.com/i.gif
18-Feb-20	Heuristic	test@xyz.com		testgroup	http://gator.com/
19-Feb-20	Heuristic	192.168.0.173	192.168.0.173	testgroupsall	http://gator.com/

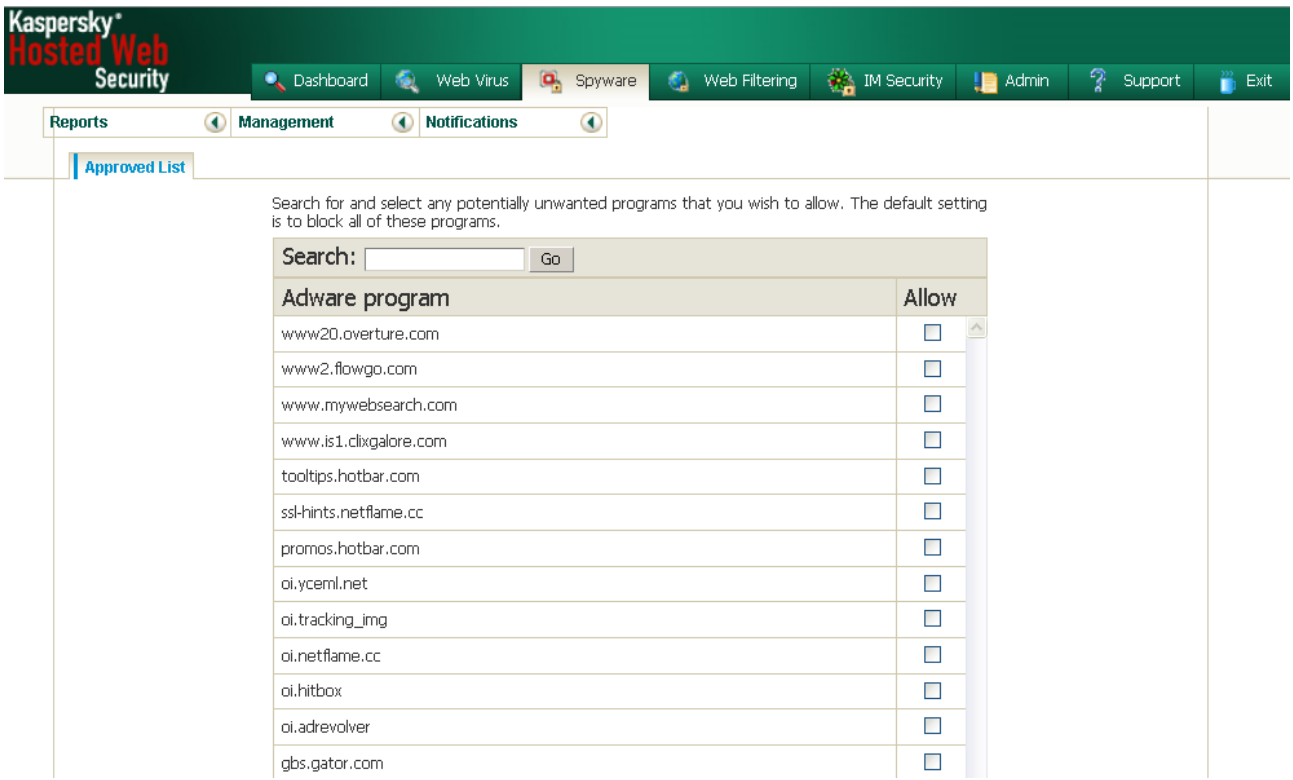
SPYWARE MANAGEMENT

Spyware Management consists of just one sub-service tab, Manage Approved List.

ADWARE PROGRAMS

By default, Kaspersky Hosted Security blocks some incoming programs that is defines as adware. If an administrator requires a specific adware application to be permitted, the administrator can simply 'check' the required adware instance/application within the Approved List. All these programs are registered in the Approved List once Kaspersky Hosted Security receives a request for its download. Therefore, it should be noted that the Approved List will expand with the scope of the organization's Web traffic.

It should be noted that all Spyware (truly malicious code, such as viruses, worms, Trojans, back-doors, key loggers, etc.) are automatically blocked by the Kaspersky Hosted Security Web Virus service. Similarly, all known Phishing exploits are automatically blocked by the Spyware service. The Adware Approved List applies to 'greyware' which typically include applications that hijack Web surfing activities, redirect users to sponsored sites, monitor non-confidential surfing habits, create unrequested pop-up ads, etc.



SPYWARE NOTIFICATIONS

Under the **Spyware Notifications** sub-service tab, there are two settings which require configuration:

- **User Messages** – specifies the message which an end-user will see when a request is blocked.
- **Email Alerts** – enables an administrator to receive an email alert whenever spyware is blocked.

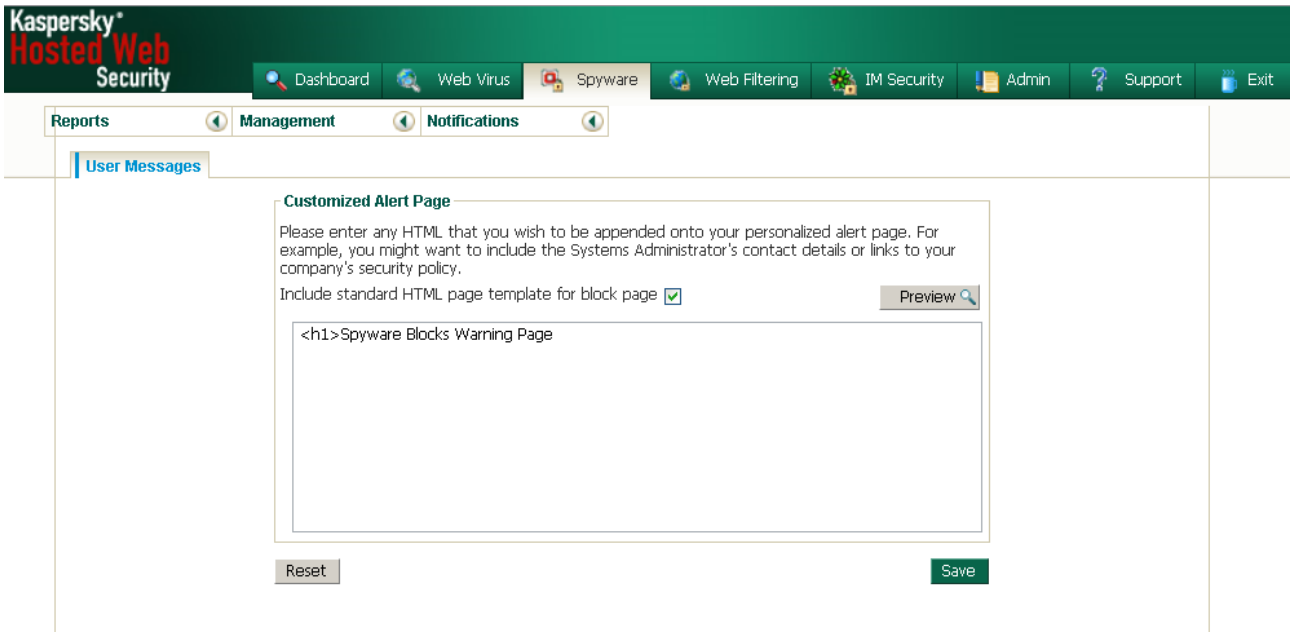
SPYWARE USER MESSAGES

The Web Security Service User Message is the page that your users will see in their Web browser if a spyware infected URL they request is blocked. In order to customize it for your organization, you can append your own information to the Default Alert Page. For example, you may wish to add the Systems Administrator's contact details, or links to your organization's security policy.

The custom information must be submitted in HTML.

Kaspersky Hosted Security allows for fully customizable block pages, which means that you can define the entire HTML output of the block page up to and including the opening and closing <html> tags. This allows you to customize block pages with your own logo and text on the block page.

1. Click the 'Spyware' service tab at the top of the screen.
2. Click the 'User Messages' button in the Notifications sub-menu. This will bring up the 'User Messages' screen.
3. Uncheck the 'Include Kaspersky Lab headers' box to remove the Kaspersky Lab logo from the block page.
4. Enter the desired HTML into the 'User Messages' field. Any images/css referenced needs to be a resolvable location. Typically you will be required to host your own images/css for this page.
5. You may insert #reason, #url, #category or #username into the HTML and it will be parsed as the reason for the block event. More detail is available in the next section.
6. Once you are happy with the Alert Page modifications you have made, click the 'Save' button located at the bottom of the screen.
7. Click the preview button just beneath the text area to see how the additional information is rendered. You must save your changes before preview displays your new settings.



USING VARIABLES TO CUSTOMIZE BLOCK PAGE TEXT

You may insert #reason, #url, #category or #username into the HTML in your custom block page and the block page will show the reason for the block event. An example below shows this more clearly:

Default block message:

```
URL contained in custom redlist default
Blocked Category : SMS / Ring Tones / Logos
EICAR-Test-File
```

Custom HTML message written by user:

```
<b>#reason<b><br>
#reason is not allowed by acme corps
```

Custom message text will appear in end-user block page:

```
<b> EICAR-Test-File<b><br>
 EICAR-Test-File is not allowed by acme corps
```

SPYWARE EMAIL ALERTS

The Spyware Email Alerts are emails that notify the administrator of incidents when a spyware application has been blocked by Kaspersky Hosted Security. The email will contain the following information:

- The IP address of the Web request that left your organization.
- The reason the requested file was blocked (malware name).
- The full URL of the Web request.

To set up Spyware Email Alerts:

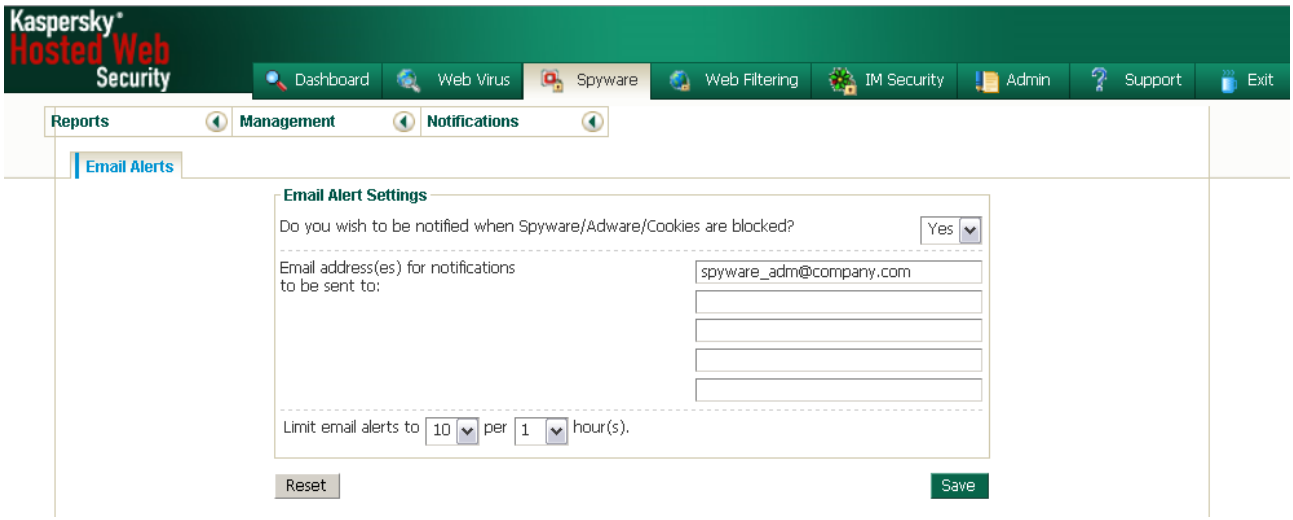
1. Click the ‘Spyware’ service at the top of the screen.
2. Click the ‘Email Alerts’ Spyware Notifications tab. This will bring up the ‘Email Alerts’ page.

3. Select whether or not you want to be notified when a spyware application is blocked by selecting 'Yes' or 'No' from the drop down box.

4. Enter the email address (or addresses) you want notifications to be sent to in the empty text fields provided. You can specify a maximum of five different email addresses where you wish to have alerts sent. If you require the alerts to be sent to more addresses than this, we recommend that you set up a group mailing address.

5. If you wish to throttle the number of email alerts you receive, click in the box next to the statement 'Limit these alerts to'. Throttling will now be activated and you must then select the number of alerts you wish to receive for the given number of hours you specify. For example: you might decide that you only want to receive a maximum of three email alerts in any two-hour period.

6. To save the settings and email addresses, click the 'Save' button located at the bottom of the screen.



FILTERING

The Filtering service enables you to:

- configure, enforce, and monitor Web content filtering for your organization;
- view comprehensive, filtering related information in the form of statistical reports, graphs, tables and exportable data files, based on your Web traffic and filtering blocks;
- customize the HTML block alert page;
- set up and manage email alerts for monitoring.

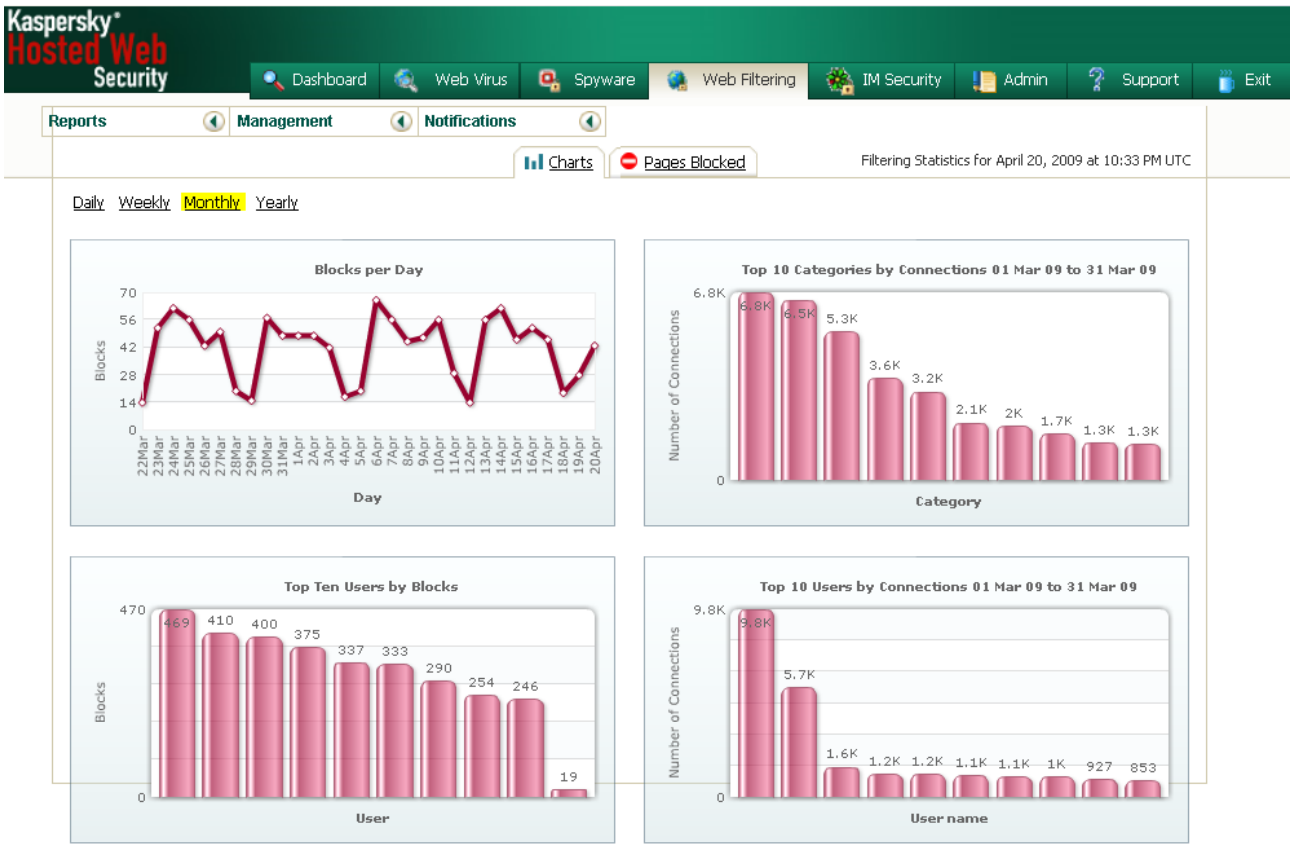
Changes made to Filtering Settings will be applied to your live Kaspersky Hosted Security filtering service within 60 seconds of submission via Kaspersky Hosted Security portal.

FILTERING DASHBOARD

The dashboard gives you a live, 'at-a-glance' view of the filtering status. To access the dashboard, click 'Web Filtering' at the top of the screen. You can select the required time scale from the top of the window: daily, weekly, monthly, or yearly.

The graphs presented are as follows:

- **Blocks per period**: this shows the number of Web requests blocked due to filtering rules for the given time period.
- **Top 10 users by Blocks**: this lists the top users by the number of blocks generated.
- **Top 10 Categories by Connection**: this lists the top requested Web filtering categories by number of connections.
- **Top 10 Users by Connection**: this lists the most active users (by directory username or IP address) by number of connections.



- **Pages Blocked (table)**: this table displays all the filtering blocks by Kaspersky Hosted Security for the given time period. The table shows 100 entries at a time and orders them by most recent. There are links at the bottom of the table to step back in lots of 100, until you reach the very first page blocked by Kaspersky Hosted Security for the given time period. For each blocked instance, the table will display:

- The date and time the page was blocked.

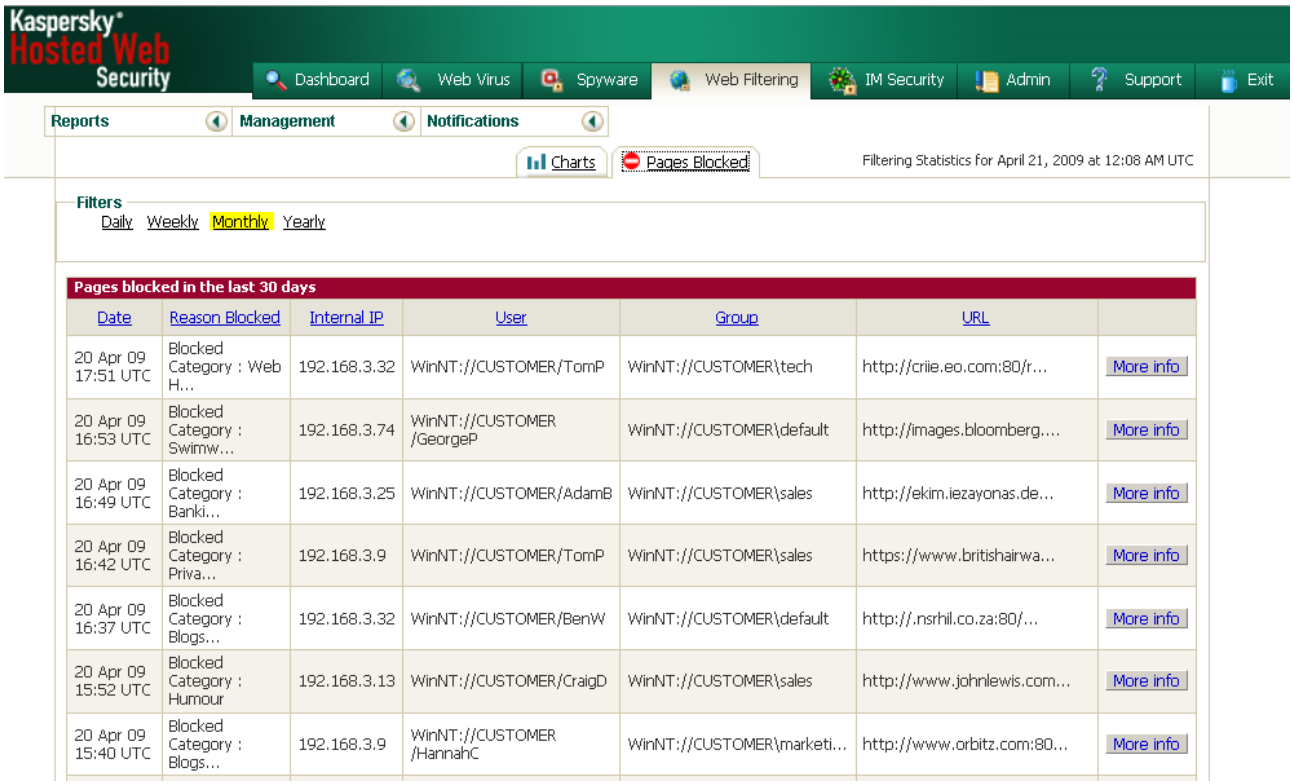
- The reason it was blocked.

- The user (internal IP address) within your organization from which the request originated.

- The user group that the originator of the request belongs to (if available, when configured through installation of a Connector).

- The URL (Uniform Resource Location) of the requested page that triggered the block.

You can also sort the table by simply clicking the corresponding column title: Date, Reason Blocked, User, Group, and URL.


Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Charts
Pages Blocked
Filtering Statistics for April 21, 2009 at 12:08 AM UTC
Filters
Daily Weekly Monthly Yearly
Pages blocked in the last 30 days
Date | Reason Blocked | Internal IP | User | Group | URL
20 Apr 09 17:51 UTC | Blocked Category : Web H... | 192.168.3.32 | WinNT://CUSTOMER/TomP | WinNT://CUSTOMER\tech | http://criie.eo.com:80/r... | More info
20 Apr 09 16:53 UTC | Blocked Category : Swimw... | 192.168.3.74 | WinNT://CUSTOMER /GeorgeP | WinNT://CUSTOMER\default | http://images.bloomberg.... | More info
20 Apr 09 16:49 UTC | Blocked Category : Banki... | 192.168.3.25 | WinNT://CUSTOMER/AdamB | WinNT://CUSTOMER\sales | http://ekim.iezayonas.de... | More info
20 Apr 09 16:42 UTC | Blocked Category : Priva... | 192.168.3.9 | WinNT://CUSTOMER/TomP | WinNT://CUSTOMER\sales | https://www.britishairwa... | More info
20 Apr 09 16:37 UTC | Blocked Category : Blogs... | 192.168.3.32 | WinNT://CUSTOMER/BenW | WinNT://CUSTOMER\default | http://.nsrhil.co.za:80/... | More info
20 Apr 09 15:52 UTC | Blocked Category : Humour | 192.168.3.13 | WinNT://CUSTOMER/CraigD | WinNT://CUSTOMER\sales | http://www.johnlewis.com... | More info
20 Apr 09 15:40 UTC | Blocked Category : Blogs... | 192.168.3.9 | WinNT://CUSTOMER /HannahC | WinNT://CUSTOMER\marketi... | http://www.orbitz.com:80... | More info

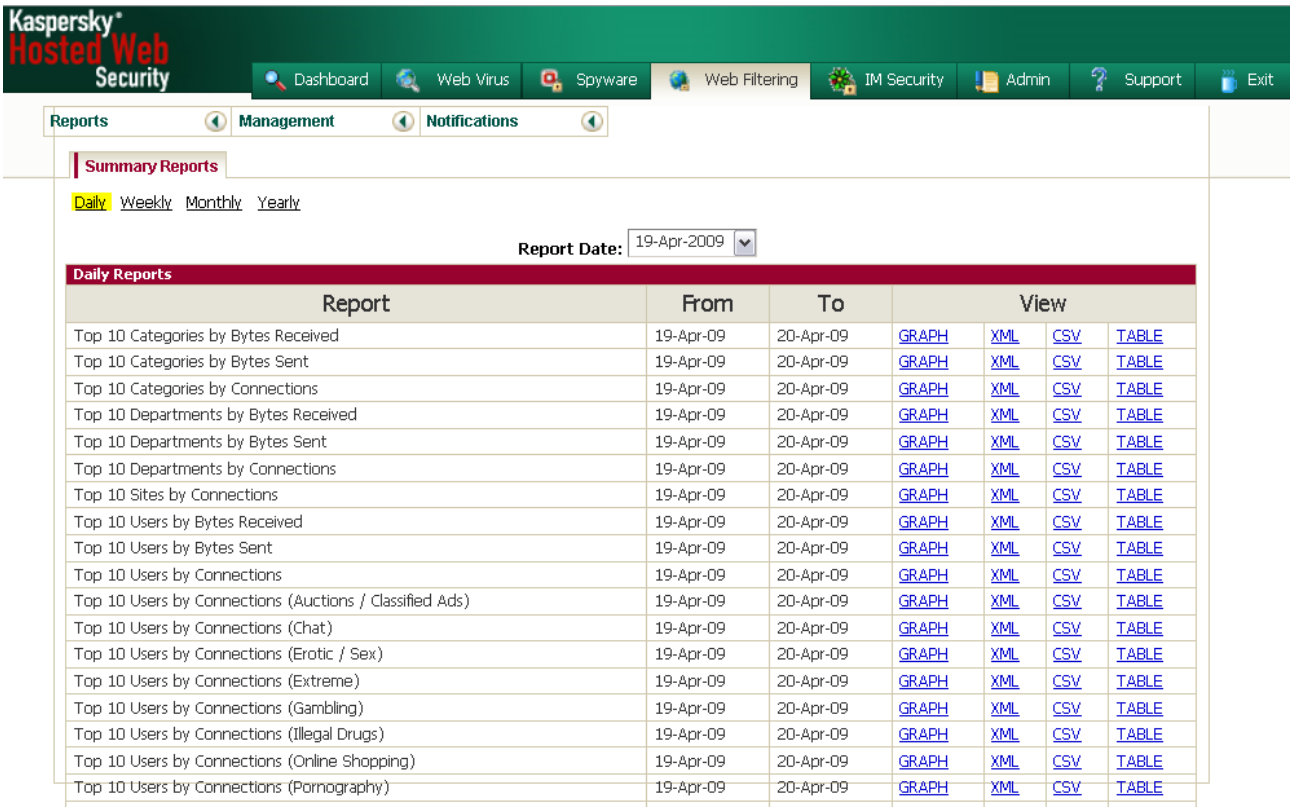
FILTERING REPORTS

There are three different types of reporting available:

- Summary Reports
- Scheduled Reports
- Forensic Audit Reports

FILTERING SUMMARY REPORTS

This feature provides a Filtering Summary Report which is available either as a table, graph or exportable file. The exportable files are provided for those who wish to import the reports data into their own reporting applications. They are available in two formats: CSV (Comma Separated Value) and XML (Extensible Mark-up Language). The current version of Kaspersky Hosted Security currently has 29 different reports, which are generated once a day from the Internet traffic your organization generates within a 24-hour period. The reports come in daily, weekly, monthly and yearly formats, allowing you to view the trends, patterns and characteristics of your organization's Web usage over time. This information can be used to help formulate the type of restrictions to apply within your organization and in modifying or fine-tuning your current restrictions.


Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Summary Reports
Daily
Weekly
Monthly
Yearly
Report Date: 19-Apr-2009
Daily Reports
Report
From
To
View
Top 10 Categories by Bytes Received 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Categories by Bytes Sent 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Categories by Connections 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Departments by Bytes Received 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Departments by Bytes Sent 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Departments by Connections 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Sites by Connections 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Bytes Received 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Bytes Sent 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections (Auctions / Classified Ads) 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections (Chat) 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections (Erotic / Sex) 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections (Extreme) 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections (Gambling) 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections (Illegal Drugs) 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections (Online Shopping) 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE
Top 10 Users by Connections (Pornography) 19-Apr-09 20-Apr-09 GRAPH XML CSV TABLE

Report Descriptions:

REPORT NAME	DESCRIPTION	GRAPH TYPE
Bytes Received by Hour	The number of bytes downloaded by the hour	Bar
Bytes Sent by Hour	The number of bytes uploaded by the hour	Bar
Connections per Hour	The number of requests for files by the hour	Bar
Top 10 Categories by Bytes Received	The top 10 Web content categories based on bytes downloaded	Bar
Top 10 Categories by Bytes Sent	The top 10 Web content categories based on bytes uploaded	Bar
Top 10 Categories by Connections	The top 10 Web content categories based on the number of files requested	Bar
Top 10 Groups by Bytes Received	The top 10 user groups based on bytes downloaded	Pie
Top 10 Groups by Bytes Sent	The top 10 user groups based on bytes uploaded	Pie
Top 10 Groups by Connections	The top 10 user groups based on the number of files requested	Pie
Top 10 Pages by Bytes Received	The top 10 specific Web pages based on bytes downloaded	Bar
Top 10 Pages by Bytes Sent	The top 10 specific Web pages based on bytes uploaded	Bar
Top 10 Pages by Connections	The top 10 most visited Web pages based on how many times they were requested.	Bar
Top 10 Sites by Bytes Received	The top 10 sites (based on domain names, i.e. microsoft.com) by bytes downloaded	Bar
Top 10 Sites by Bytes Sent	The top 10 sites (based on domain names, i.e. microsoft.com) by bytes uploaded	Bar
Top 10 Sites by Connections	The top 10 sites (based on domain names, i.e. microsoft.com) by the number of requests made	Bar
Top 10 Users by Bytes Received	The top 10 individual users based on how many bytes they have downloaded	Pie
Top 10 Users by Bytes Sent	The top 10 individual users based on how many bytes they have uploaded	Pie

REPORT NAME	DESCRIPTION	GRAPH TYPE
Top 10 Users by Connections	The top 10 individual users based on how many requests they have generated through browsing	Pie
Top 10 Users by Connections (Auctions / Classified Ads)	The top 10 individual users based on how many requests they have made to Auctions / Classified Ads Web sites	Bar
Top 10 Users by Connections (Chat)	The top 10 individual users based on how many requests they have made to Chat sites	Bar
Top 10 Users by Connections (Erotic / Sex)	The top 10 individual users based on how many requests they have made to Erotic / Sex Web sites	Bar
Top 10 Users by Connections (Extreme)	The top 10 individual users based on how many requests they have made to Extreme sites	Bar
Top 10 Users by Connections (Gambling)	The top 10 individual users based on how many requests they have made to Gambling sites	Bar
Top 10 Users by Connections (Illegal Drugs)	The top 10 individual users based on how many requests they have made to Illegal Drugs sites	Bar
Top 10 Users by Connections (Online Shopping)	The top 10 individual users based on how many requests they have made to Online Shopping sites	Bar
Top 10 Users by Connections (Pornography)	The top 10 individual users based on how many requests they have made to Pornography sites	Bar
Top 10 Users by Connections (Sports)	The top 10 individual users based on how many requests they have made to Sports sites	Bar
Top 10 Users by Connections (Travel)	The top 10 individual users based on how many requests they have made to Travel sites	Bar
Top 10 Users by Connections (Web Mail)	The top 10 individual users based on how many requests they have made to Web Mail sites	Bar

VIEWING THE REPORTS

1. Click the 'Web Filtering' service tab at the top of the screen.
2. Click the 'Reports' link and select 'Summary Reports'.
3. Select the required reporting period from the top of the page (Daily, Weekly, Monthly or Yearly).
4. From the pull-down list, select the end date for the reporting period.
5. To view a specific report, simply click the 'Graph' button located just to the right of the report's name, underneath the 'View' heading. This will open up a separate window for displaying the graph.
6. If you wish to view a report in table format, simply click the 'Table' button instead. This will open up a separate window to display the Table.
7. To download the report data in either CSV or XML format, simply click the 'CSV' or 'XML' buttons. You will then be prompted by your browser to specify a save location for the data file.

FILTERING SCHEDULED REPORTS

This feature provides Web Filtering scheduled reporting, available either as a table, graph or both. You can select the type of presentation, report date range, users to report on, the report generation scheduled, formatting options, and who to email the report to. Kaspersky Hosted Security generates this report once a day from the Internet traffic that your organization sends within a 24-hour period.

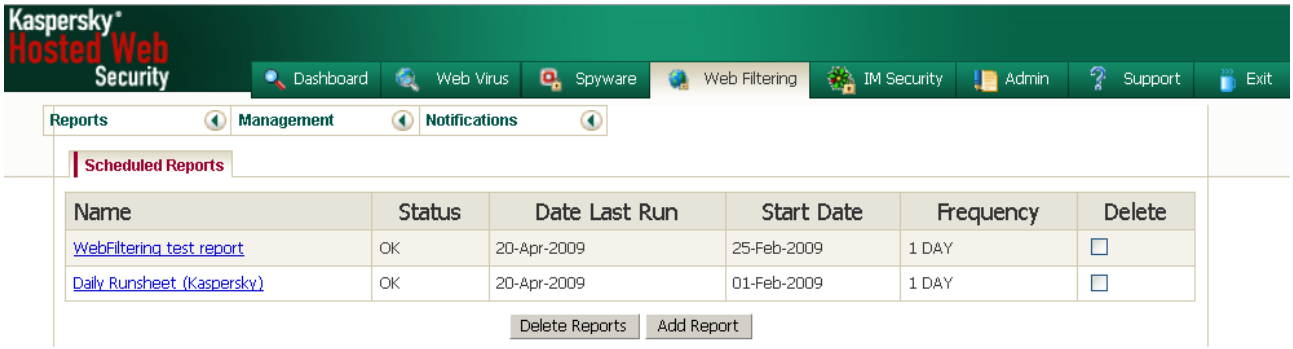
1. Edit an existing Web Filtering Scheduled Report.
2. Click the 'Web Filtering' service tab at the top of the screen.

3. Click the 'Scheduled Reports' link and select 'Scheduled Reports'.

4. From the Filtering Scheduled Reports page, you can click available reports by clicking their name, which is underlined as a link, to edit the report.

5. The report will allow you to change all options, except that the presentations that were previously selected are not editable. If you wish to change the presentations you wish to report upon, you should create a new scheduled report.

6. Once you have finished editing the existing scheduled report, click the 'Update Report' button to save your changes.



DELETE AN EXISTING WEB FILTERING SCHEDULED REPORT

1. Click the 'Web Filtering' service tab at the top of the screen.

2. Click the 'Scheduled Reports' link in the 'Reports' sub-service tab.

3. From the Web Filtering Scheduled Reports page, you can click the checkbox to the right of the available reports, and then click the 'Delete Reports' button to delete the selected reports. A validation message will appear to ask if you are sure you want to delete the selected reports. Click 'OK' to delete the reports.

ADD A WEB FILTERING SCHEDULED REPORT

1. Click the 'Web Filtering' service tab at the top of the screen.

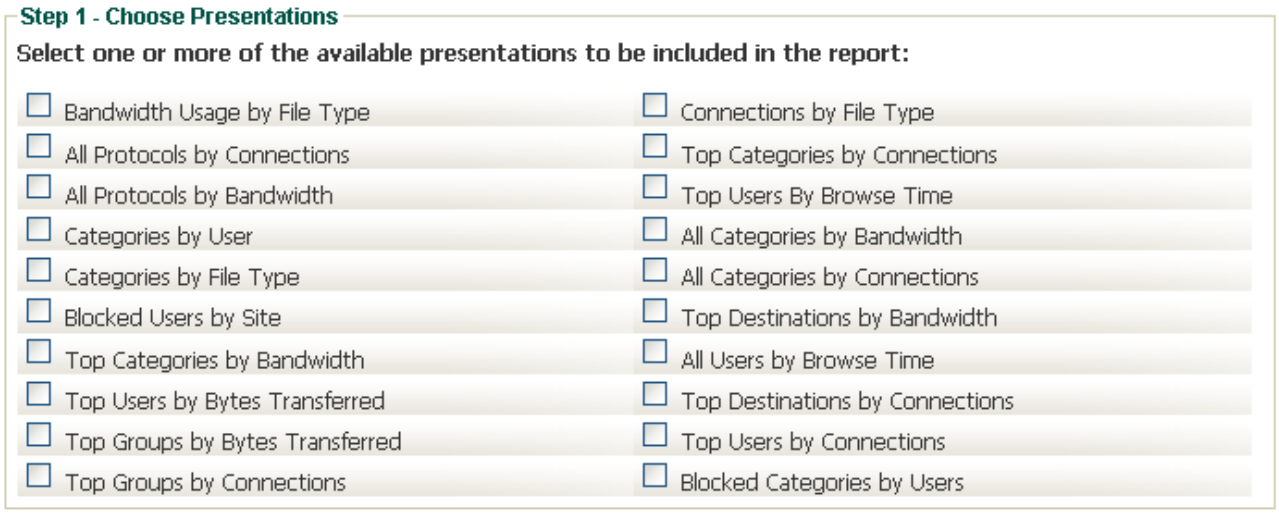
2. Click the 'Reports' link and select 'Scheduled Reports'.

3. From the Filtering Scheduled Reports page:

    - **Step 1**: Select from the available presentations to be included in the report:

        - Top Destinations by Number of Hits
        - All Protocols by Bandwidth
        - All Categories by Number of Hits
        - Top Categories by Connections
        - All Categories by Bandwidth
        - Top Groups by Number of Hits
        - URLs per User
        - Top Users by Bytes Transferred

- All Protocols by Connections
- Users by Categories
- File Types by User
- Top Users by No of Hits
- File Types by Connections
- Categories by User
- File Types by Bandwidth
- Top Destinations by Bandwidth
- Top Groups by Bytes Transferred
- Top Categories by Bandwidth


Step 1 - Choose Presentations
Select one or more of the available presentations to be included in the report:
Bandwidth Usage by File Type
All Protocols by Connections
All Protocols by Bandwidth
Categories by User
Categories by File Type
Blocked Users by Site
Top Categories by Bandwidth
Top Users by Bytes Transferred
Top Groups by Bytes Transferred
Top Groups by Connections
Connections by File Type
Top Categories by Connections
Top Users By Browse Time
All Categories by Bandwidth
All Categories by Connections
Top Destinations by Bandwidth
All Users by Browse Time
Top Destinations by Connections
Top Users by Connections
Blocked Categories by Users

Throughout the day, Kaspersky Hosted Security counts the length of time each user downloads data through the Web browser. This counter stops after 4 minutes of inactivity from the user. Any further browsing will append to the current amount of time for the 24 hour period.

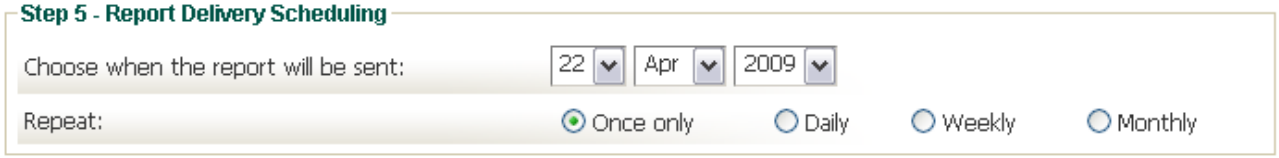
- **Step 2**: Select the desired date range required: either Yesterday, Last full week, Last full month or a customized date range.

- **Step 3**: Select either all users or specific users or groups by clicking the 'Edit' button. The Groups and User IPs screen show the available groups and User or IP addresses that are available to be reported on. This data is based on the monitored traffic.

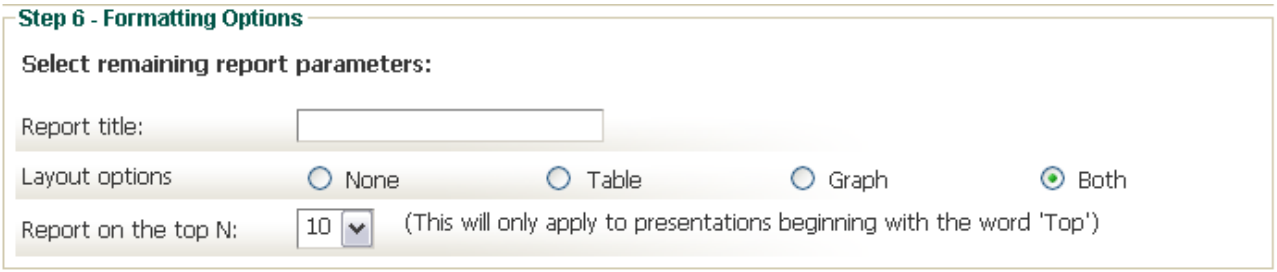
You can filter on either groups or user (not a combination of both). Clicking the Add group or Add user button will bring up a popup where you can select them, When you save, only the open filter (group or user) will be saved.

- **Step 4**: For those reports that are based on categories, you can select a subset of these categories to report on. You can select multiple categories for the filter. The default option is to report on all traffic accessed, whether that is a Web page the user has clicked on, or images/files within the Web page. You can select to filter the report so that only pages which the user has clicked for are displayed, by clicking the 'Display HTTP Webpages only' filter.

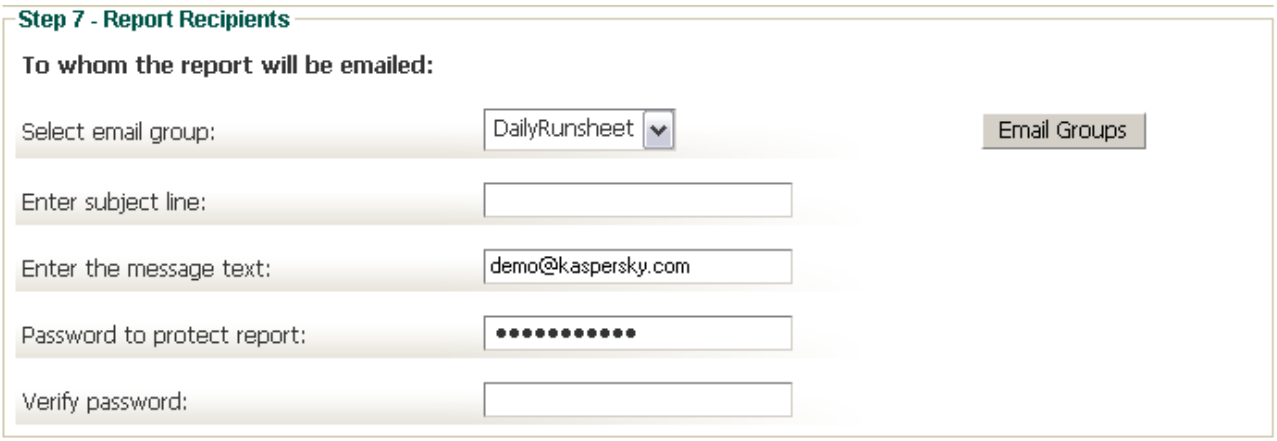
- Step 5: Schedule the report delivery by selecting the specific start date using the drop down boxes and selecting the frequency of the scheduled report delivery – either Once only, Daily, Every 7 days, or Every 30 days.



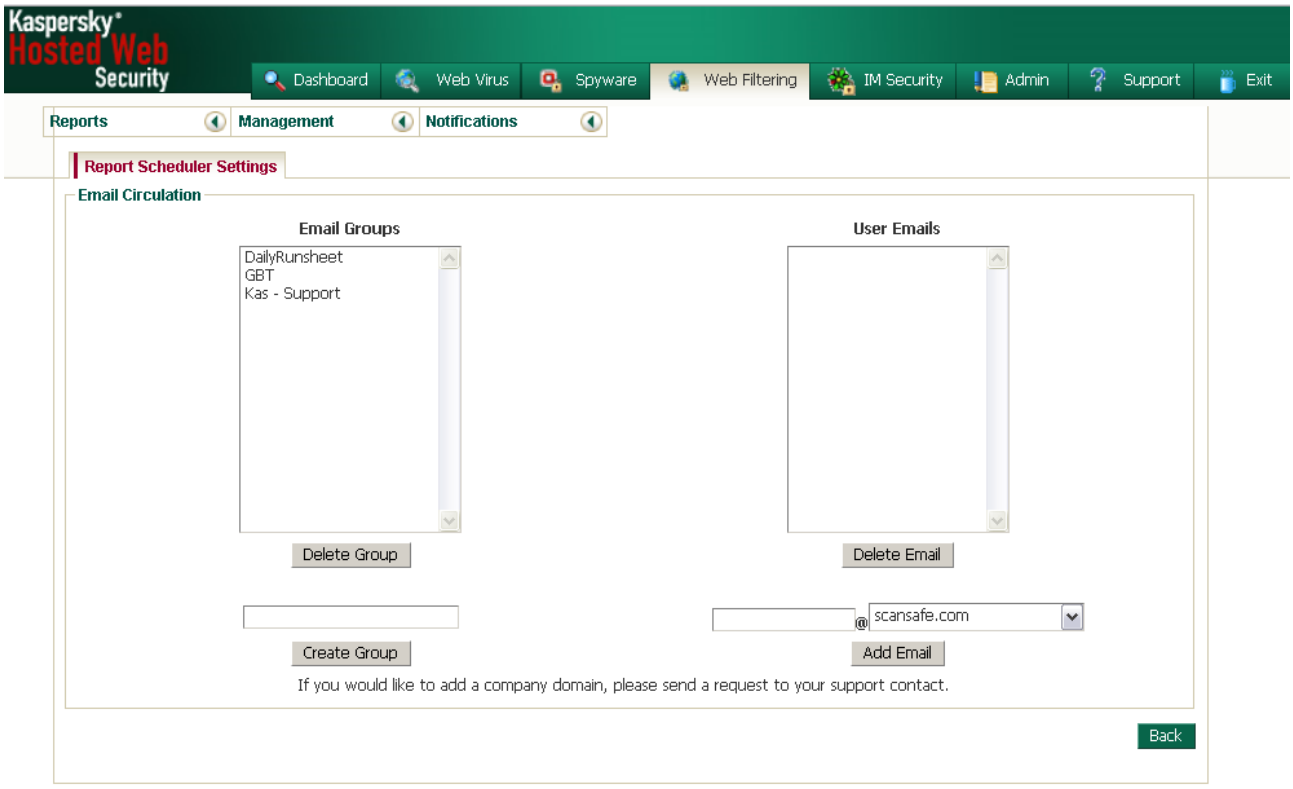
- Step 6: Select formatting options for the report (including typing in a report title) and layout options by selecting a table or graph presentation or both. You may also select the top 'N' (number) for the presentations you have selected, such as the 'Top 50 Categories by Connections'.



- **Step 7**: Select the report recipients by selecting the email group, entering the subject line of the email, the message text and a password to open and review the report. If you want to create new email groups or edit existing ones, click the 'Email Groups' button.



Select the Email Group on the left side to see the email addresses assigned to that group on the right side. You can add new email groups, delete groups, and remove and add email addresses. Email addresses are restricted to the company domain that is created when your account is created. If you would like to add additional company domains, please send a request to KHSS-Support@kaspersky.com. Click the 'Back' button to return to the previous screen. Click the 'Activate Report' button when you have finished.



FILTERING FORENSIC AUDIT

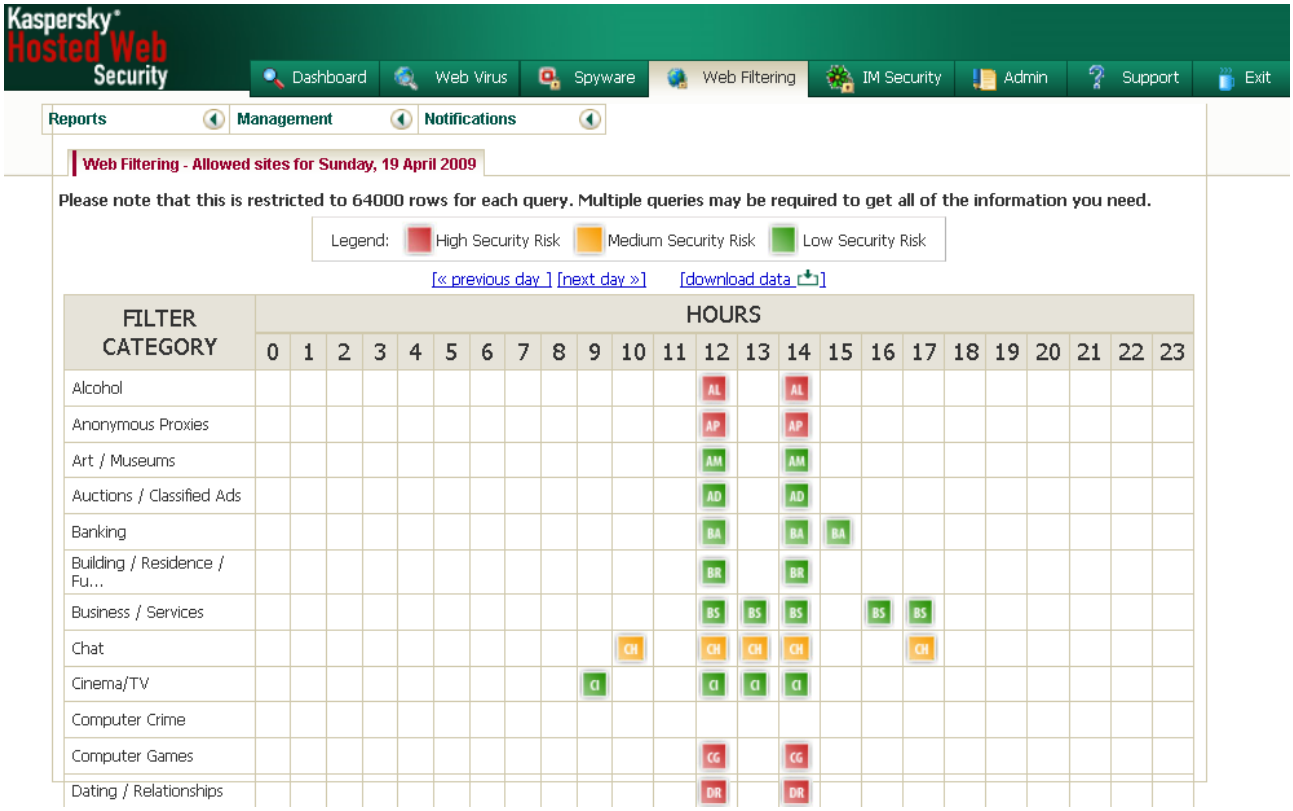
The Forensic Audit sub-service enables an administrator to receive a detailed audit trail of all filtering activity resulting in a blocked Web request. The requested activity is then either viewable as a summary report for allowed traffic or exported to a CSV file for blocked traffic.

ALLOWED TRAFFIC

The Web Filtering Allowed Traffic sub-service displays all Web traffic that has not been blocked for either all users or a specific user over the period of a day. The result is a graphical display of the allowed traffic per category over the period of a day. You can then able to drill down and find the details of the sites accessed within a specific category. The results are exported into a CSV file. To enable easy of viewing data over a period of time, you can navigate by specifying a specific day.

To generate a Filtering Forensic Audit for Allowed Traffic:

1. Click the 'Filtering' service tab at the top of the screen.
2. Click the 'Forensic Audit – Allowed Traffic' button in the 'Reports' sub-service tab.
3. From the Forensic Audit page, select the desired date from the drop-down list of available days. Select who the audit is about – this can mean a specific user or the entire company. (See 'User Selection Tool' on page 17 for more information).
4. Click 'Generate Audit'.
5. The graphical display of available data by category and time will now appear.
6. To save the raw data (in CSV format) click the Download Data link, or to just download the raw data (in CSV format) for a specific category in a specific hour, click the colored square which represents this selection.

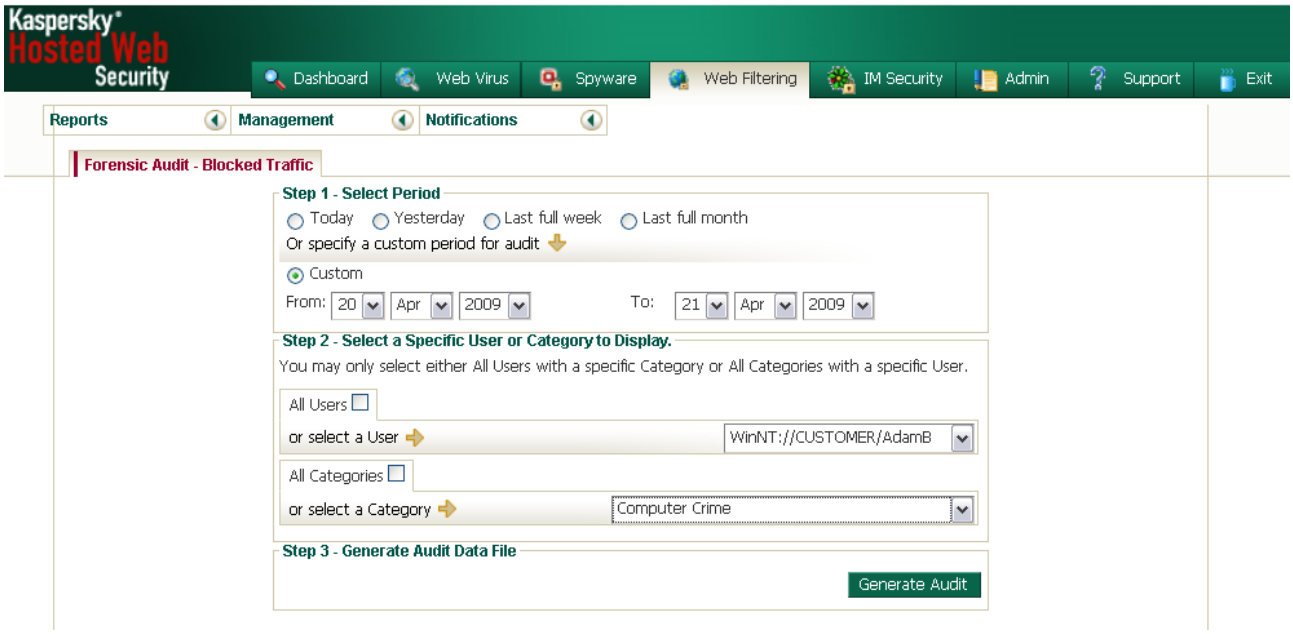

Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Web Filtering - Allowed sites for Sunday, 19 April 2009
Please note that this is restricted to 64000 rows for each query. Multiple queries may be required to get all of the information you need.
Legend: High Security Risk Medium Security Risk Low Security Risk
[« previous day] [next day »] [download data]
FILTER CATEGORY
HOURS
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Alcohol
Anonymous Proxies
Art / Museums
Auctions / Classified Ads
Banking
Building / Residence / Fu...
Business / Services
Chat
Cinema/TV
Computer Crime
Computer Games
Dating / Relationships

BLOCKED TRAFFIC

The Web Filtering Block Traffic sub-service enables an administrator to receive a detailed audit trail of all Web filtering activity resulting in a blocked Web request. The requested activity is exported to a CSV file and contains the following data:

- **Date/Time**: date and time of the blocked scan / event.
- **Threat Type**: lists the nature of the block.
- **User**: identifies the IP address of the customer site.
- **Internal IP**: identifies the internal IP address of the user.
- **Group**: identifies the directory group where the Web request originated (if available – requires installation of a Connector).

- **URL**: lists the requested URL.



The report can be generated in a similar way to the 'Allowed Traffic' report (see 'Allowed Traffic' on page 41).

Date	Threat Type	User	Internal IP	Group	URL
18-Feb-2008 15:31:31 UTC	pornography	192.168.0.173	192.168.0.173	testgroupsall	http://www.crazyhome
19-Feb-2008 10:44:43 UTC	pornography	192.168.0.173	192.168.0.173	testgroupsall	http://www.crazyhome
19-Feb-2008 10:45:44 UTC	pornography	192.168.0.173	192.168.0.173	testgroupsall	http://www.crazyhome
19-Feb-2008 10:46:20 UTC	pornography	192.168.0.173	192.168.0.173	testgroupsall	http://www.crazyhome

FILTERING MANAGEMENT

The process of configuring a Web Filtering policy requires the use of several 'filtering objects'. Each of these objects is listed under the Web Filtering Policy Manager Management sub-menu. These objects are:

- Filters
- Schedules
- Policy
- Quotas

Filters: Each Access filter itself consists of the following objects:

- Filtering Category
- Domains/URL
- Content Types
- File Types
- Exceptions

Schedules: A Schedule is a pre-defined period of time and days, based on a 7 day week and a 24 hour clock. Schedules are defined globally, but can be assigned and 're-used' within any Policy and also in the IM Control service.

Policy: A policy is a series of rules which operate in a fall-through manner, much the same way as a firewall does. Each rule is made up of a 'WHO' filter, a 'WHAT' filter and a 'WHEN' filter, alongside the action to take if this rule is matched. Rules can be active or inactive and can be reordered within the policy.

Quotas: A quota is an administrator-defined parameter which limits user Web usage, typically by time spent 'surfing' or by bytes downloaded. Quotas are defined 'globally', but are enforced by assigning them to specific polices. Please note that this functionality requires the Connector to be installed.

Each of these objects is defined specifically for each filter; however, you can copy from the default filter into other filters if you so choose.

Each of these objects will be discussed in further detail below.

FILTERS

In Kaspersky Hosted Security, a 'Filter' is a set of user-defined Web filtering components. These components will have an action associated with them in the Policy rule (e.g. either Allow or Block). These filters are broken down into five different components:

- **Categories**: These are presented as a selectable list of all the different categories that a website might fall under, for example Sports, Music, Pornography, Online Shopping etc. Through the use of categories you can quickly select a wide range of websites simply by clicking a check box next to each category you wish to include in your rule.

- **Domains/URL**: this is a list of websites in relation to the particular policy rule which contains them. A common use for this is to create a global allowed list and a global blocked list.

- **Content Types**: These relate to the content that is specified in the header of the HTTP request. A normal Web page will usually have a content type of 'text/html'; this is also known as a MIME type (Multipurpose Internet Mail Extension). Another example of the many different MIME types is 'application/PDF'; when a Web browser sees this, it will try to start up a suitable application in order to display a PDF file. Common MIME types are listed in this section, and you can also add your own custom types.

- **File Types**: These relate to all the various types of files which a user might try to download via links in a Web page, each one distinguished by its file extension. For example, a file with the '.exe' extension is a Microsoft Windows executable file, or a file with a '.mp3' extension is an encoded sound file. So if you chose to block all files with an '.exe' extension, then if a user tried to go to the following URL: http://www.games.com/arcade/invaders.exe they would receive a message saying that the requested file has been blocked. A further check is also made on the 'Content Disposition' header if this is present in the response. Common file extensions are listed in this section, and you can also add your own custom extensions.

- **Exceptions**: Any website on this list will cause the rule to fall through to the next rule on the list.

CREATING A NEW FILTER

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.

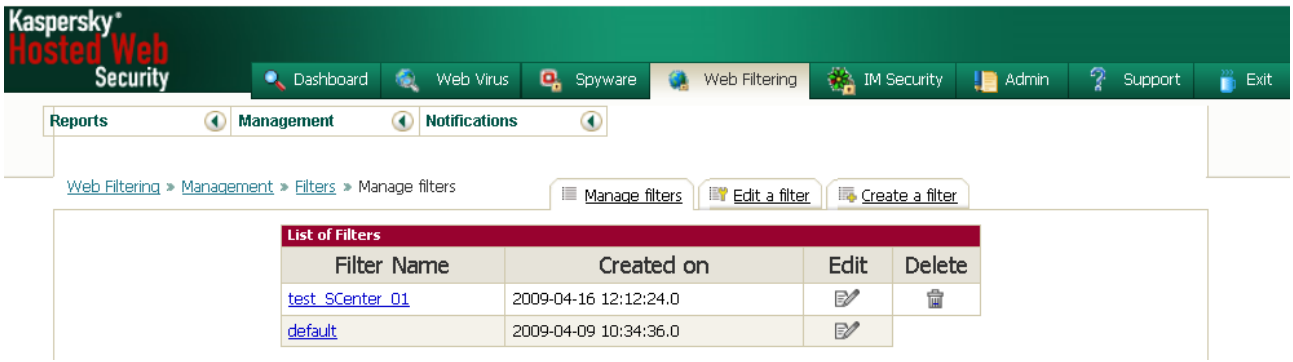
2. Under the Management sub-service dropdown, click the 'Filter'. This will bring up the 'Manage Filter' screen.

3. The main 'Manage Filters' page presents you with a listing of all your current filters. To create a new filter, click the 'Create a Filter' tab.

4. Enter the name of the new filter in the box 'Filter Name' text field.

5. Edit each one of the Web filtering components, then click the 'Save' button at the lower right-hand corner. You will then see your new filter added to the 'List of filters'.

6. The name of the new Filter will now appear in the Filters page.



EDITING OR VIEWING A FILTER

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.

2. Under the Management sub-service dropdown, click the 'Filter'. This will bring up the 'Manage Filter' screen.

3. The main 'Manage Filters' page presents you with a list of all your current filters. To review the settings for a particular filter, click the restriction name in question or click the 'Edit' button. The components of the requested Restriction will then appear. You can also click the 'Edit a Filter' tab and select the filter you wish to edit from the Name dropdown list.

4. You can now click the tabs for each of the components (Categories, Domains/URL, Content Types, File Types, and Exceptions). It is recommended that you configure each component in series, starting at the top of the menu. If separate HTTP/HTTPS Filtering is enabled (see 'Global Settings' on page 60), two tabs will appear here instead of 'Categories'. Clicking the HTTP tab will take you to the HTTP filters page; clicking the HTTPS tab will take you to the HTTPS filters page.

CATEGORIES. CONFIGURING THE WEB CATEGORIES YOU WOULD LIKE SELECTED

1. Make sure you have selected the required filter you wish to edit. You can verify the filter you are editing because its name is listed at the top of the page in the 'Filter name' box.

2. Click the Categories tab. This will bring up the 'Select Categories' page.

3. Click the boxes next to the corresponding categories which you want to select.

4. If you want to select all the available categories, you can click the 'Select All' button located at the bottom of the page. Conversely, you can click the 'Deselect All' box to remove all category selections.

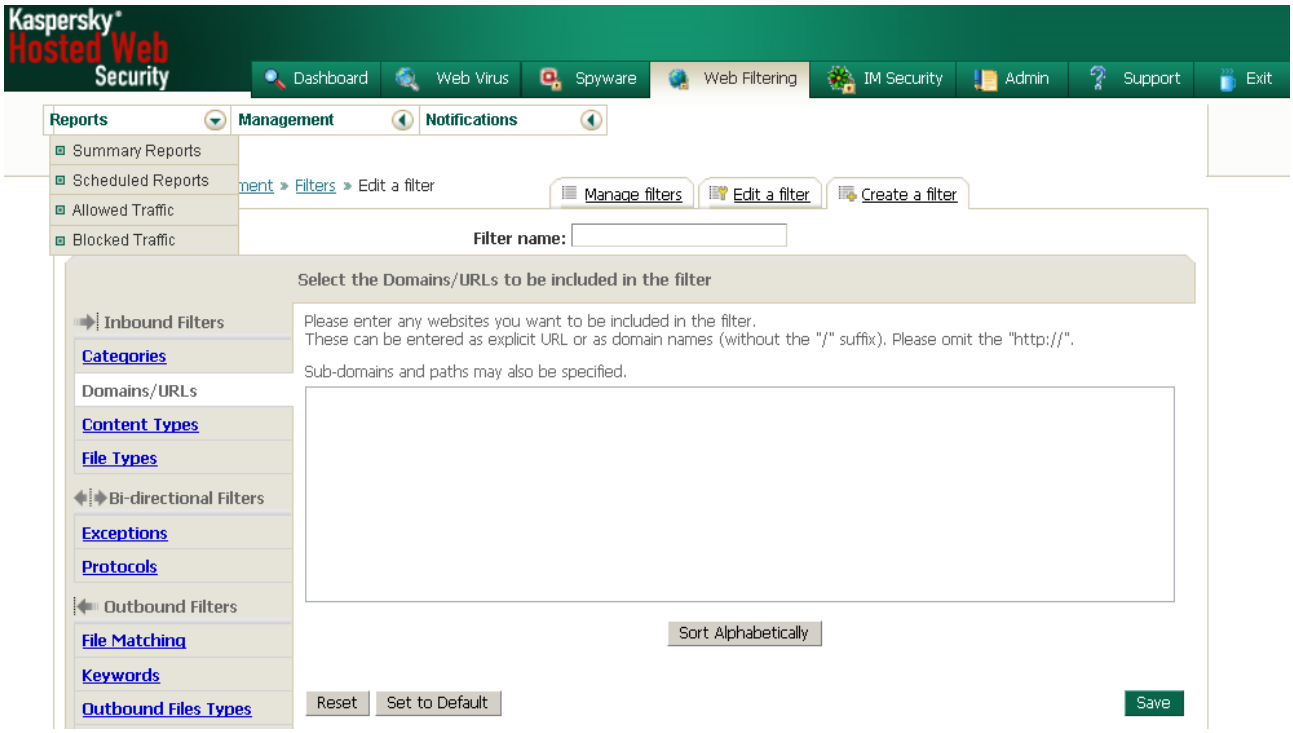
5. Click the 'Save' button at the bottom of the screen to save your changes.

   It is possible to have separate category selections for both HTTP (unencrypted) and HTTPS (encrypted) Web traffic. This would allow you, for instance, to allow access to unencrypted gambling sites, but block all encrypted gambling sites.

DOMAINS/URLS. CONFIGURING THE DOMAIN/URLS LIST

1. Make sure you have selected the required filter you wish to edit.

2. Click the button 'Domains/URL' tab. This will bring up the 'Define Domains/URL' page.



3. In the text area provided you may enter a Web site in two different ways:

   - By entering the explicit URL minus the 'http://' (e.g. www.bbc.co.uk/news)
   - By entering a domain (e.g. bbc.co.uk).

   Please note that each entry must be put on a new line and there should be no trailing slash '/' at the end of the URL. Also, you should not include the 'www.' with the entry, otherwise related sub-domains will be excluded.

4. To make viewing of your listed pages easier, you can click the 'sort alphabetically' button at the bottom of the text area.

5. To recall the Domains/URL entries from the Default Filter, click the 'Set to Default' link. This may be useful for quickly configuring new filters which are typically just modifications of the Default set of filters.

6. Once you are satisfied with the Domains/URL entries, click the 'Save' button located at the bottom of the page.

   Clicking 'Reset' will reset the list back to the saved list.

CONTENT TYPES. CONFIGURING THE CONTENT TYPES YOU WOULD LIKE TO FILTER

1. Verify that you have selected the particular Filter you wish to edit.

2. Click the 'Content Types' tab. This will bring up the 'Content Types' page.

3. Click the boxes corresponding to the content types which you want to filter on. A check mark indicates that the Content Type will be filtered.

4. If you wish to filter on all the available content types, then you can click the 'Select All' check box located in each section. This will place a check mark for every content type in that section. A second click the 'Select All' check box will allow all content types for that section. Alternatively, you can click the 'Select All' button at the bottom of the page to filter on all content in all sections. Clicking the 'Deselect All' button at the bottom of the page will remove any filters in any sections of the Content Type page.

5. If you wish to enter your own custom content types, you can type these into the 'Custom' text area. The content types must be entered using the same syntax as the following example: application/msword. Please note that all entries must be on a separate line.

6. You can sort your list of custom content types alphabetically by clicking the 'Sort alphabetically' option directly underneath the text area.

7. The 'Set to Default' button copies the settings from the Default Filter, making it easier and quicker to configure new filters.

8. Once you are satisfied with the content types you wish to filter on, click the 'Save' button located at the bottom of the screen. Clicking the 'Cancel' button will return you to the previous page without saving any of the current settings.

FILE TYPES. CONFIGURING THE FILE TYPES YOU WOULD LIKE TO FILTER

1. Verify that you have selected the particular filter you wish to edit.

2. Click the 'File Types' tab on the left hand side. This will bring up the 'File Types' page.

3. Click in the boxes next to the corresponding file extensions to which you want to filter on. A check mark indicates that the File Type will be filtered.

4. If you wish to filter all the available file extensions, then you can click the 'Select All' button located in the bottom of the page. This will place a check mark for every file extension. A second click the 'Deselect All' button will remove the filter on all content types.

5. If you wish to enter your own custom file extensions, you can type these into the 'other file extensions' text box area. The file extensions must be entered using the same syntax as the following example:

   tif

   aac

   psd

   Please note that all entries must be on a separate line. File extensions must not have a '.' (period) in front.

6. You can sort your list of custom content types alphabetically by clicking the 'Sort alphabetically' option directly underneath the text area.

7. The 'Set to Default' button copies the settings from the Default Restriction, making it easier and quicker to configure new filters.

8. Once you are satisfied with the content types you wish to filter on, click the 'Save' button located at the bottom of the screen. Clicking the 'Cancel' button will return you to the previous page without saving any of the current settings.

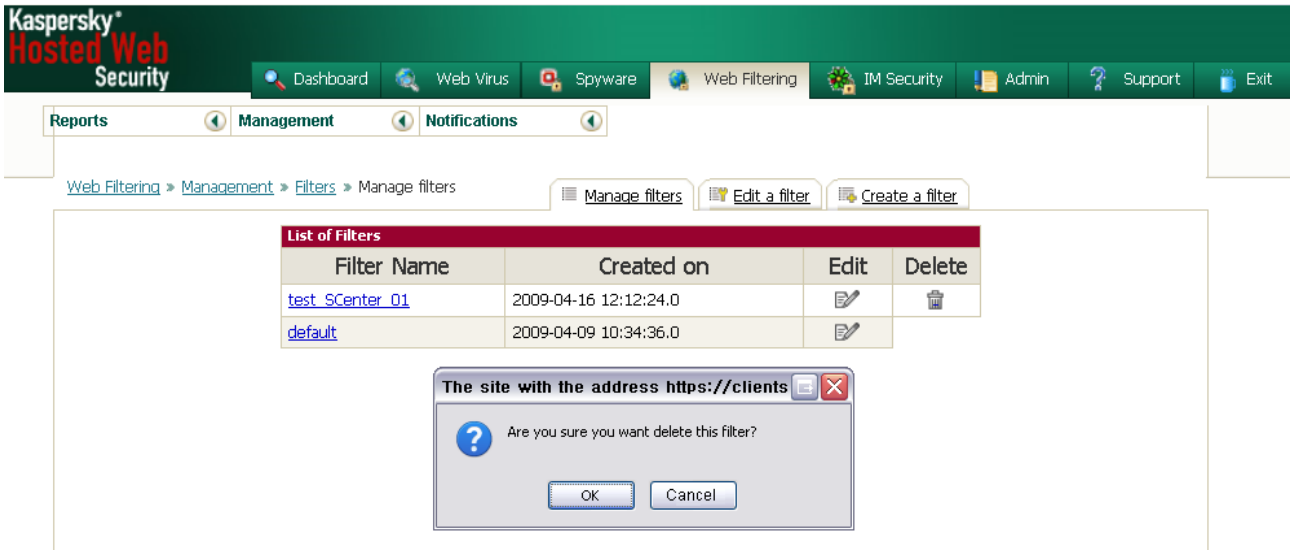
DELETING A FILTER

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.

2. On the Management sub-menu click the 'Filters'. This will bring up the main 'Filters' page.

3. The main 'Filters' page presents you with a listing of all your current filters. In order to delete one of these, click the 'Delete' icon located to the right of the desired filter.

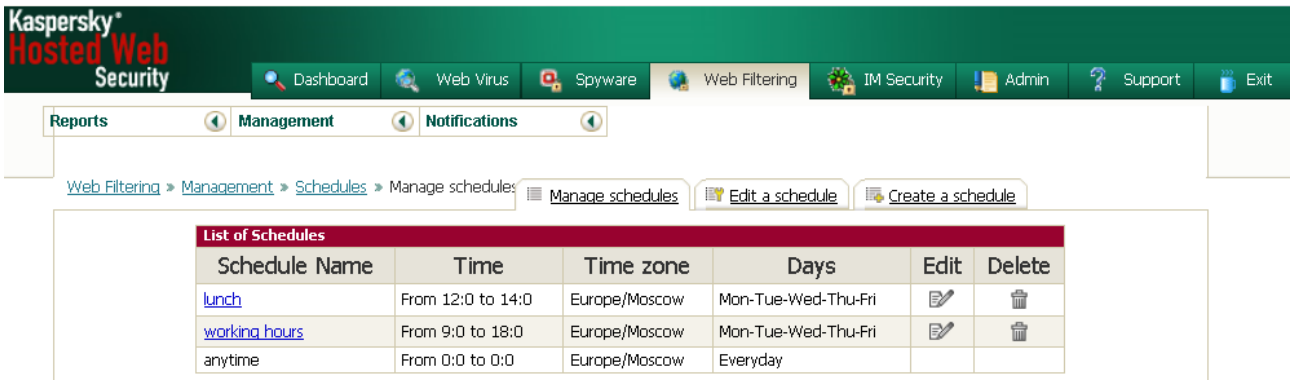
4. A dialog box will appear asking if you are sure you want to delete the filter. Click the 'OK' button to proceed with deletion. The deleted filter will no longer be displayed in the list on the main 'Filters' page.



If the filter you have chosen to delete has one or more pairings associated with it in the Policy rules, then Kaspersky Hosted Security will not let you delete it. You must first delete the dependent policy rule, and then delete the filter.

SCHEDULES

When implementing Web filtering within an organization, you may wish to change the type of rules a group of users has based on the time of day and/or day of the week. For example, you might like to let your staff have access to Internet banking, online shopping and news sites only during their lunch hour. Schedules within Kaspersky Hosted Security facilitate this by enabling you to create a time period (called a Schedule) and then pair that 'Schedule' with a particular Group and 'Filter' within the 'Policy'. In this way, a Group can have many different types of Web access depending on the time of day and day of the week.



HOW KASPERSKY HOSTED SECURITY PROCESSES SCHEDULES

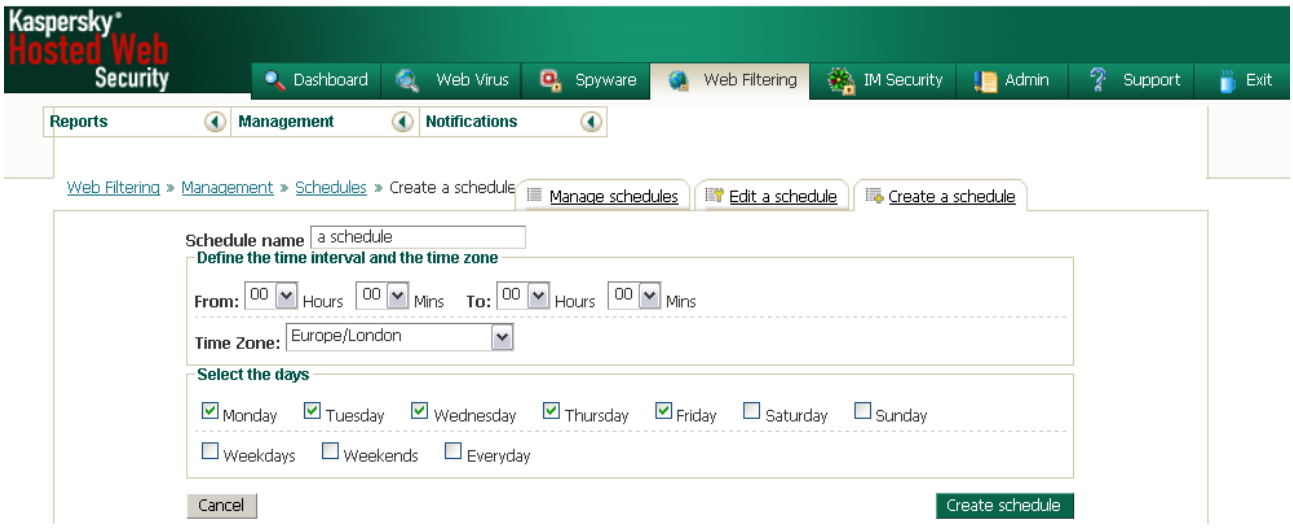
Within Kaspersky Hosted Security a schedule takes precedence based on the position of the rule with the policy. For example, suppose that you have three schedules:

- Default (24x7)
- Work Day (09:00 – 18:00)
- Lunch (13:00 – 14:00)

If you were to add a rule which had the Work Day schedule with Group A above another rule with the Lunch schedule against Group A, the first rule will process and if the filter is matched the action will take place regardless of whether the Lunch schedule would have made a difference. To stop this from happening, you should therefore always place rules with shorter time periods in the schedules above those with longer schedules.

CREATING A SCHEDULE

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.
2. Click the 'Schedules' link in the 'Management' sub-service menu. This will bring up the main 'Manage Schedules' page.
3. The 'Manage Schedules' page presents you with a listing of all your current Schedules. To create a new Schedule, click the 'Create a Schedule' tab at the top of the page.
4. Type the name you wish to give to the new Schedule in the 'Schedule name:' text field located at the top of the page.
5. Select the 'From' and 'To' times that you would like the Schedule to encompass, by selecting the hour and or minutes from the respective drop-down boxes provided.



If you would like to create a 24-hour Schedule, then you must set both the 'From' and 'To' times to 00hrs 00mins.

6. Select the time zone for which you would like to set up this Schedule.

7. Select the days of the week for which you would like the Schedule to be active. This is done by clicking the check boxes located next to each day of the week. If you click the Weekdays check box, Mon-Fri will be selected, if you click the Weekends check box, Sat-Sun will be selected and if you click the Everyday check box Mon-Sun will be selected.

You cannot create a Schedule without selecting at least one day of the week.

8. Once you are happy with the settings for your new Schedule, click the 'Save' bottom located at the bottom of the page.

EDITING A SCHEDULE

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.

2. Click the 'Schedules' link in the 'Management' sub-service menu. This will bring up the main 'Manage Schedules' page.

3. The main 'Manage Schedules' page presents you with a listing of all your current Schedules. There are three ways to edit an existing Schedule:

   - Click the name of the Schedule.
   - Click the 'Edit' icon to the right of the Schedule details.
   - Click the 'Edit a Schedule' tab and select the Schedule from the drop-down list.

4. Modify the settings of the Schedule and click 'Save' to save the configuration. You will be returned to the Manage Schedules tab. Otherwise, click the 'Cancel' button to abort and to return to the Manage Schedules tab.

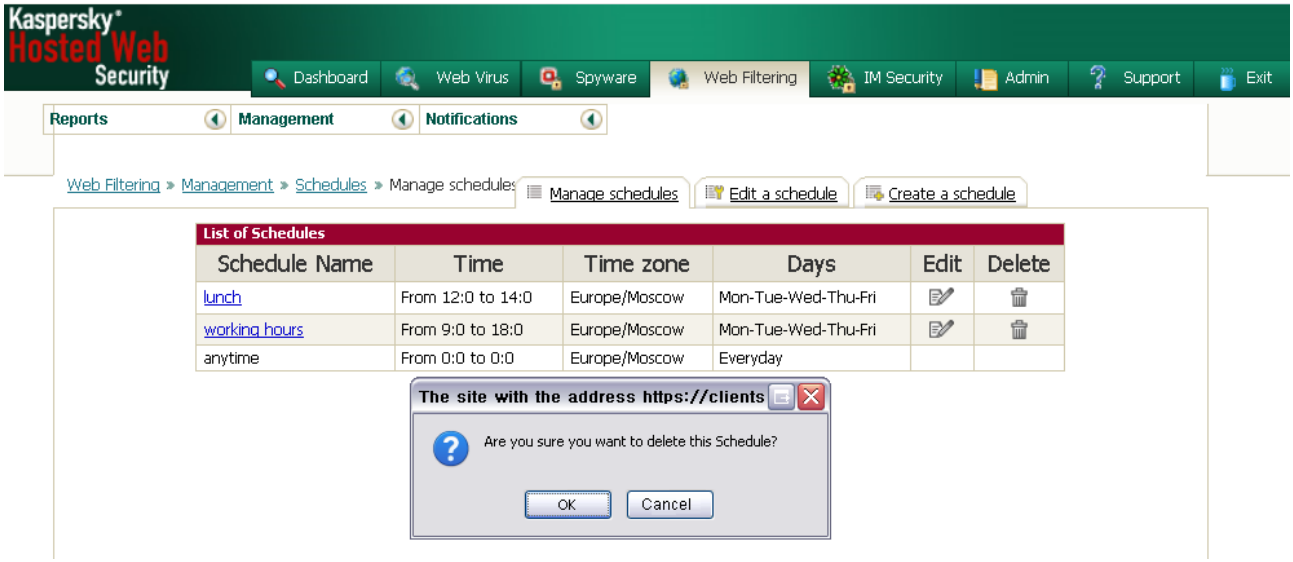
DELETING A SCHEDULE

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.

2. Click the 'Schedules' link in the 'Management' sub-service menu. This will bring up the main 'Manage Schedules' page.

3. The main 'Manage Schedules' page presents you with a listing of all your current Schedules. To delete an existing Schedule, click the corresponding check box next to an existing Schedule and click the 'Delete Schedules' button.

4. The deleted Schedule will no longer be displayed in the list on the main 'Schedules' page.



If the Schedule you have chosen to delete has one or more pairings associated with it in the Policy rules, then Kaspersky Hosted Security will not let you delete it.

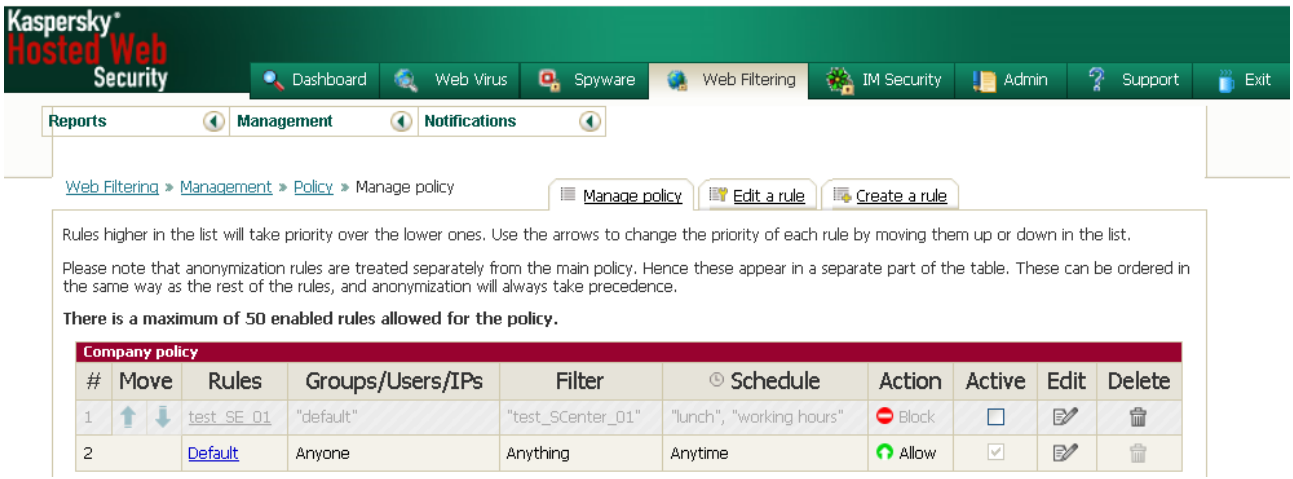
POLICY

The Policy sub-service tab provides you with a visual overview of the Filtering Rules you have configured for your organization and a means to add more in an ordered manner. The simple layout enables you to see all the User Groups and their applied filtering rules. Each combination of a Filter and a Schedule within the Policies page is referred to as a Pairing. Each Policy Rule must consist of at least one pairing. To create a typical, time-dependent policy, multiple pairings can be used.

ADDING OR EDITING A POLICY RULE

1. Click the 'Web Filtering' service on the main navigation bar at the top of the screen.

2. Click the 'Policy' link under the 'Management' sub-service menu.


Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Web Filtering » Management » Policy » Manage policy
Manage policy
Edit a rule
Create a rule
Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.
Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.
There is a maximum of 50 enabled rules allowed for the policy.
Company policy
Move Rules Groups/Users/IPs Filter Schedule Action Active Edit Delete
1 test_SE_01 "default" "test_SCenter_01" "lunch", "working hours" Block
2 Default Anyone Anything Anytime Allow

3. Click the 'Create a Rule' tab located at the top of the page. You will then be taken to the 'Create a Rule' page. This page allows you create a new rule in the policy.

4. The first thing you need to do is give it a unique name in the 'Name:' field.

5. You should now choose which action is going to take place when this rule is matched. Currently you have the choice of three actions:

   - Block
   - Allow
   - Anonymize
   - Warn

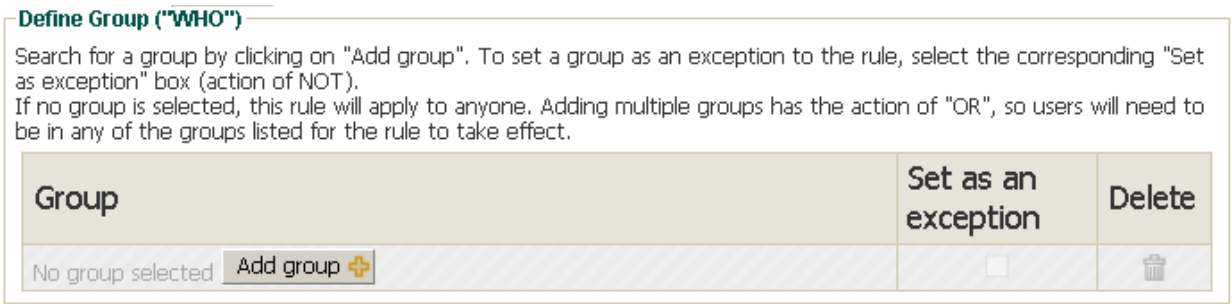
   'Block' will prevent the filtered users from downloading this content, and the block page will be displayed.

   'Allow' will allow the filtered users to download this content and proceed normally.

   'Anonymize' will remove the user details from ALL Web filtering records (needed in some countries to comply with local law). Please note that all Anonymize rules will appear in their own section at the top of the Company Policy rule list, but these can be reordered within the anonymized rules.

   'Warn' can be used for HTTP only. This function will redirect the end user to the Warn Alert page where they can accept the responsibility to visiting the domain.

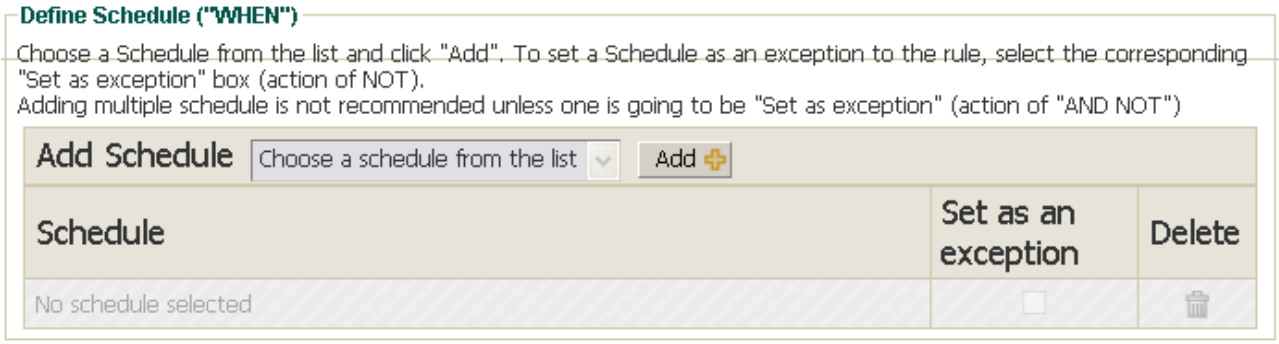
6. You then need to define 'WHO' this rule is going to run against. Leaving this blank will cause this filter to be applied against anyone. You can add in individual groups by clicking the 'Add Group' button. This will cause the Select Group screen to become visible.


Define Group ("WHO")
Search for a group by clicking on "Add group". To set a group as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).
If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.
Group
Set as an exception
Delete
No group selected
Add group

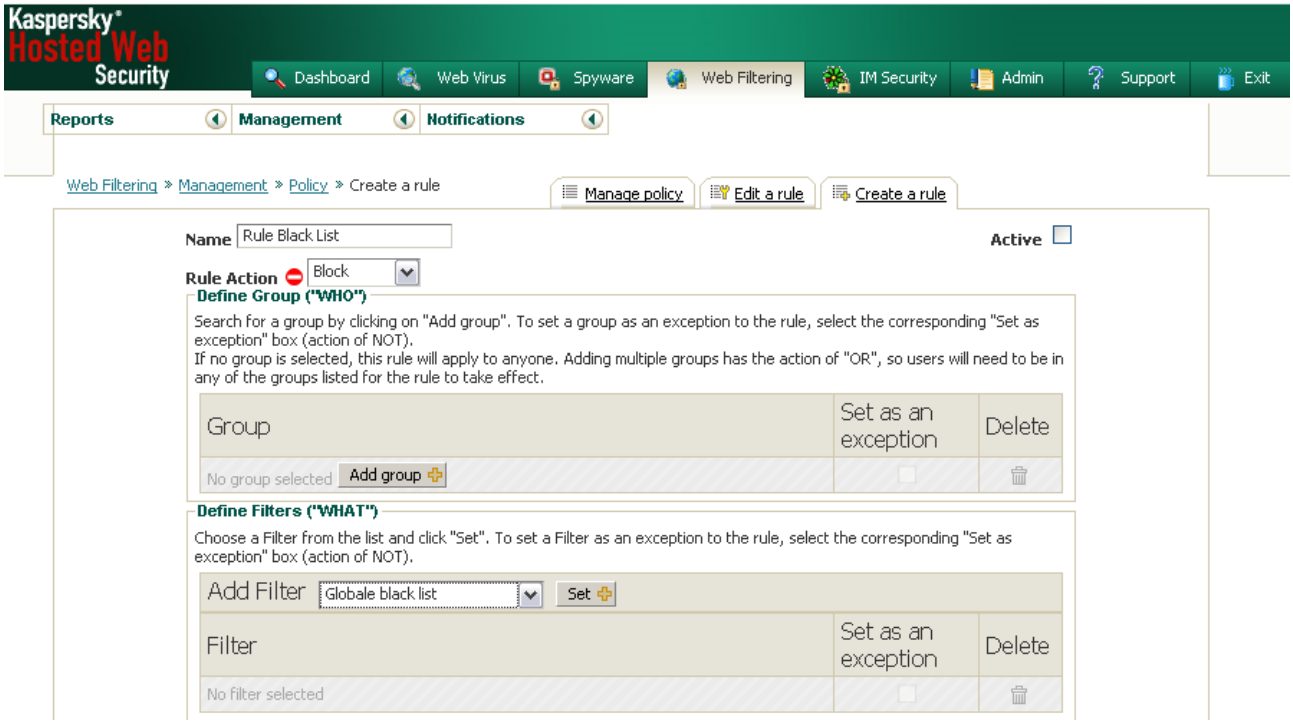
7. You can find the group you are looking for by entering the group name (or part of) in the search box and clicking the 'Go' button. You can also list all of the groups starting with a particular character by clicking the # (for symbols or numbers) or the letters at the top of the Search Groups screen.

8. Once you can see the group you want, click the 'Select' button and then click the 'Confirm Selection' button to return to the rule with the group added to the rule.

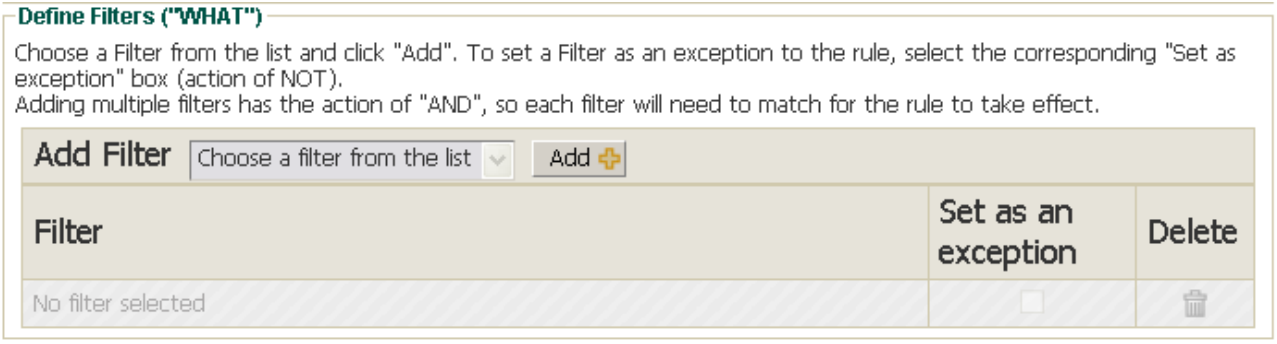
9. Clicking the 'Go' button with an empty search box will return a list of all groups registered against your company.


Define Schedule ("WHEN")
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as exception" (action of "AND NOT")
Add Schedule
Choose a schedule from the list
Add
Schedule
Set as an exception
Delete
No schedule selected

10. You then need to define 'WHAT' this rule will filter on. You can select any of your filters from the drop down box and click the Add button. Adding more than one filter will have the action of 'ANDing' the filters together. You can make the filter into a NOT action by clicking the 'Set as an exception' check box. (If you do this with only one filter, it becomes a 'NOT', if it is a second filter, then it becomes an 'AND NOT').


Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Web Filtering » Management » Policy » Create a rule
Manage policy
Edit a rule
Create a rule
Name
Rule Black List
Active
Rule Action
Block
Define Group ("WHO")
Search for a group by clicking on "Add group". To set a group as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).
If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.
Group
Set as an exception
Delete
No group selected
Add group
Define Filters ("WHAT")
Choose a Filter from the list and click "Set". To set a Filter as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).
Add Filter
Globale black list
Set
Filter
Set as an exception
Delete
No filter selected

11. You then need to define 'WHEN' this rule will be in effect. By default a new rule has the anytime schedule, but you can delete this and add in another by selecting it from the list. If you add in any more schedules these should be exceptioned as 'AND NOTs', as any schedules added after the first one will 'AND' the schedules together.

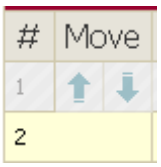

Define Filters ("WHAT")
Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).
Adding multiple filters has the action of "AND", so each filter will need to match for the rule to take effect.
Add Filter
Choose a filter from the list
Add
Filter
Set as an exception
Delete
No filter selected

12. Click 'Create Rule' to save the pairings to return to the Manage Policy window. Unless you have checked the 'Active' checkbox, the rule will be inactive (grayed out). You can now move the rule into the correct position using the up and down arrows on the left hand side of the rule. Once it is in the correct position, you can click the active check box and apply the changes.

ORDERING THE RULES

The Company policy works in much the same way as a firewall. The Anonymize rules will appear at the top of the list of rules and the anonymize action will be remembered for any user which matches these rules further down the list.

All other rules can be ordered beneath these. To change the order of the rules, use the up and down arrows to reposition the rules.



We recommend that you put the rules which are in effect for the smallest time periods at the top of the rules.

ACTIVE/INACTIVE RULES

It is possible to make a rule active or inactive in the policy. All inactive rules will have no impact on the traffic and can be moved around within the policy without any changes to the way traffic is filtered.

On the company rules list, each rule (except Default which is always active) has a check box to say if the rule is active. Inactive rules are also grayed out in the rules list.

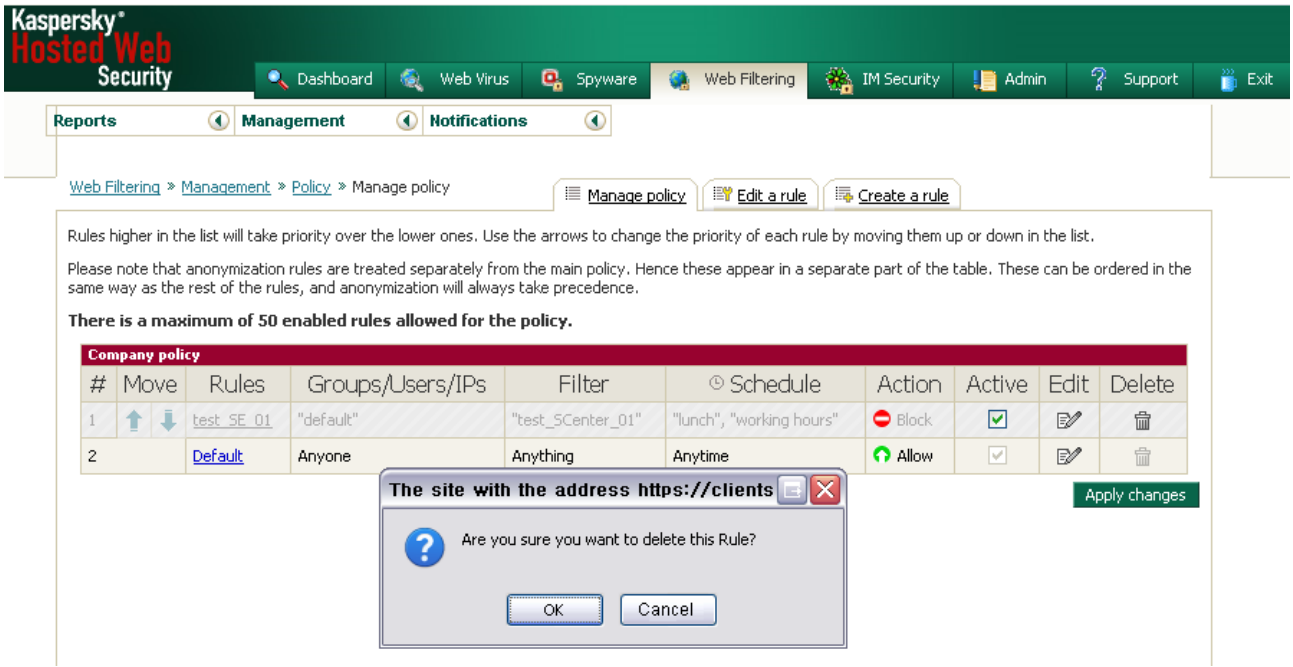
To make an active rule inactive you should clear the Active check box and then click 'Apply Changes'.

To make an inactive rule active, you should check the Active check box and then click 'Apply Changes'.

All new rules are added into the policy just above the default rule and are always inactive unless you clicked on the active check box when you created the rule.

DELETING A RULE

1. Click the 'Web Filtering' tab on the main navigation bar at the top of the screen.
2. Click the 'Policy' link in the 'Management' sub-service menu. This will then bring up the main 'Manage Policy' page.
3. Find the Rule within the listed Policy that you want to delete, and then click the 'Delete' Button located to the right of the pairing.
4. You will then be presented with a pop-up dialog box asking you if you are sure you want to delete the rule. Click the 'OK' button to proceed.
5. You should now see that the rule is no longer listed in the 'Company Policy' listing.

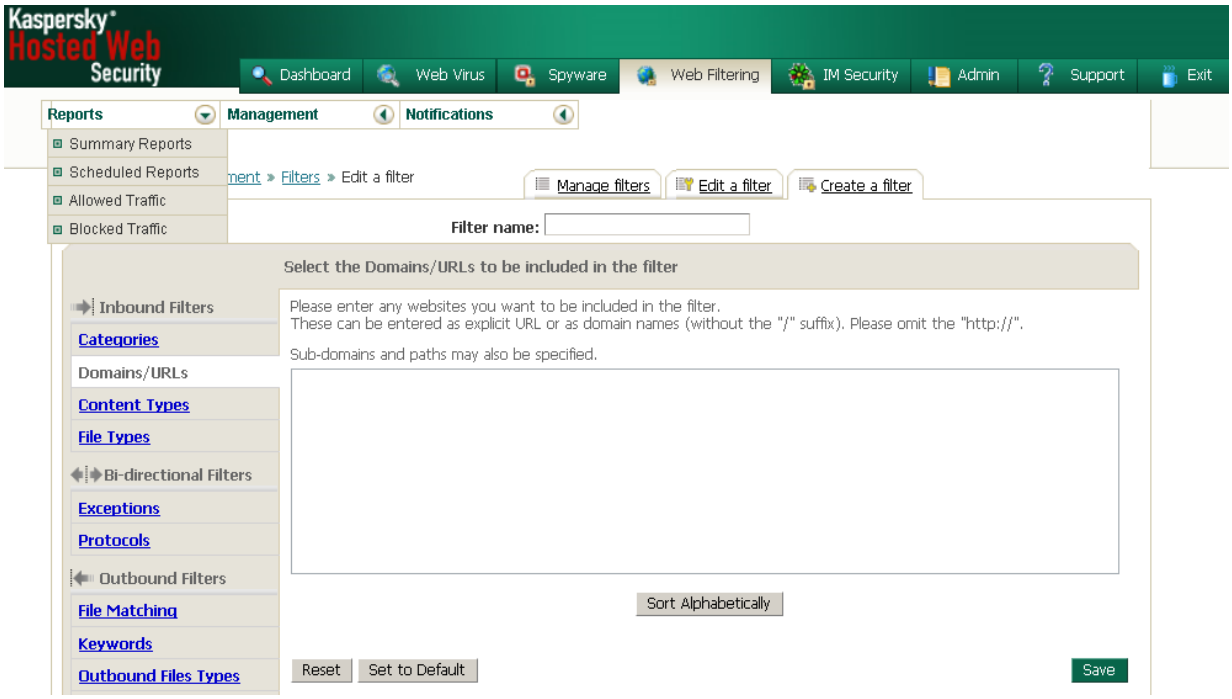

Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Web Filtering » Management » Policy » Manage policy
Manage policy
Edit a rule
Create a rule
Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.
Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.
There is a maximum of 50 enabled rules allowed for the policy.
Company policy
Move Rules Groups/Users/IPs Filter Schedule Action Active Edit Delete
1 test_SE_01 "default" "test_SCenter_01" "lunch", "working hours" Block
2 Default Anyone Anything Anytime Allow
Apply changes
The site with the address https://clients
Are you sure you want to delete this Rule?
OK
Cancel

You cannot delete the default rule.

CREATING GLOBAL WHITE AND BLACK LISTS

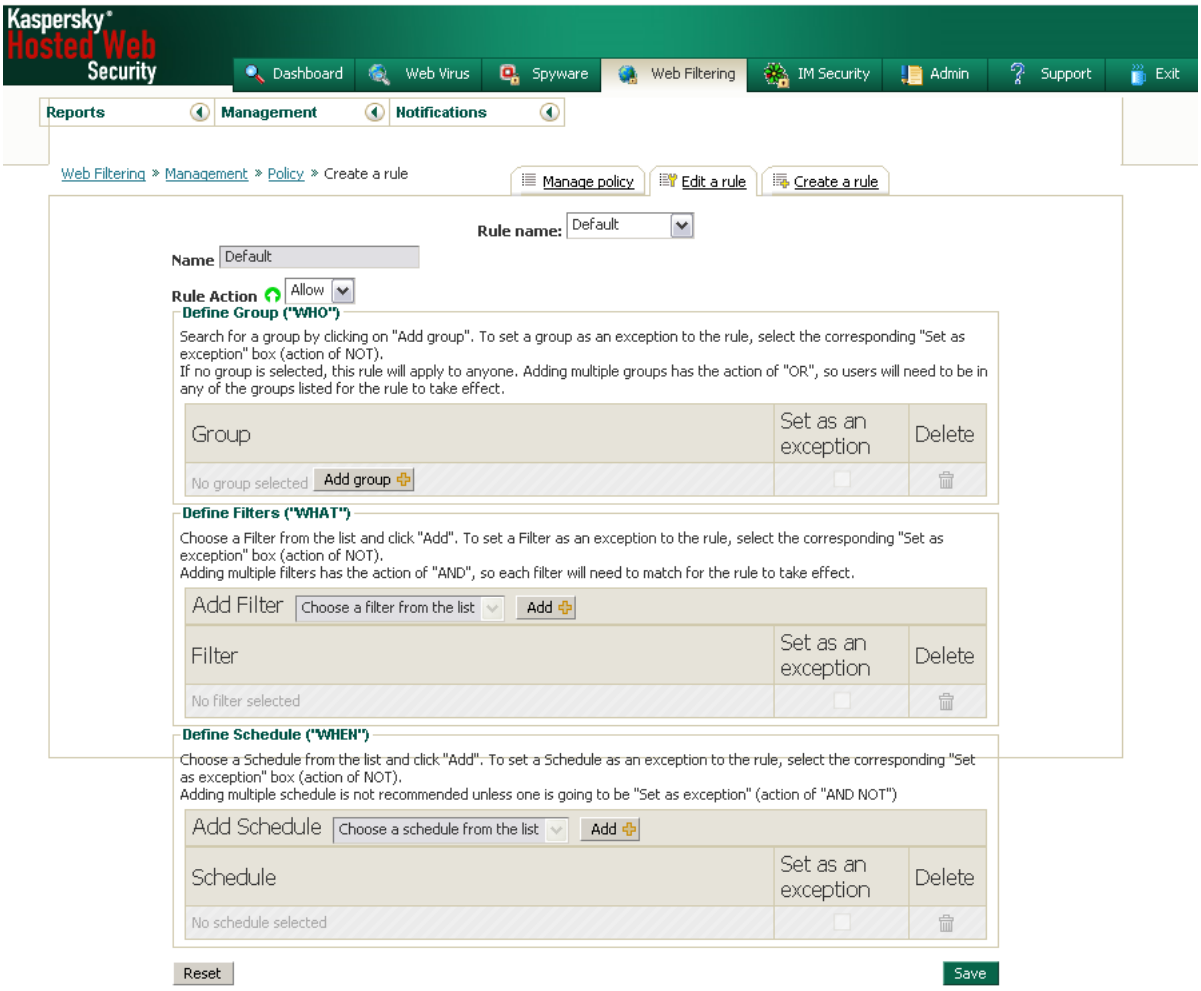
You can now create Global White and Black lists within the new policy framework. To do this, you first need to create two new filters, one called Global White List and the other called Global Black List:

1. Go to Management>Filters and click the 'Create a Filter' tab.
2. Enter 'Global White List' into the name field.
3. Click the Domains/URLs tab and enter in the URLs you wish to white list.
4. Save this new filter by clicking the 'Save' button.
5. You should now do the same for the Global Black list.

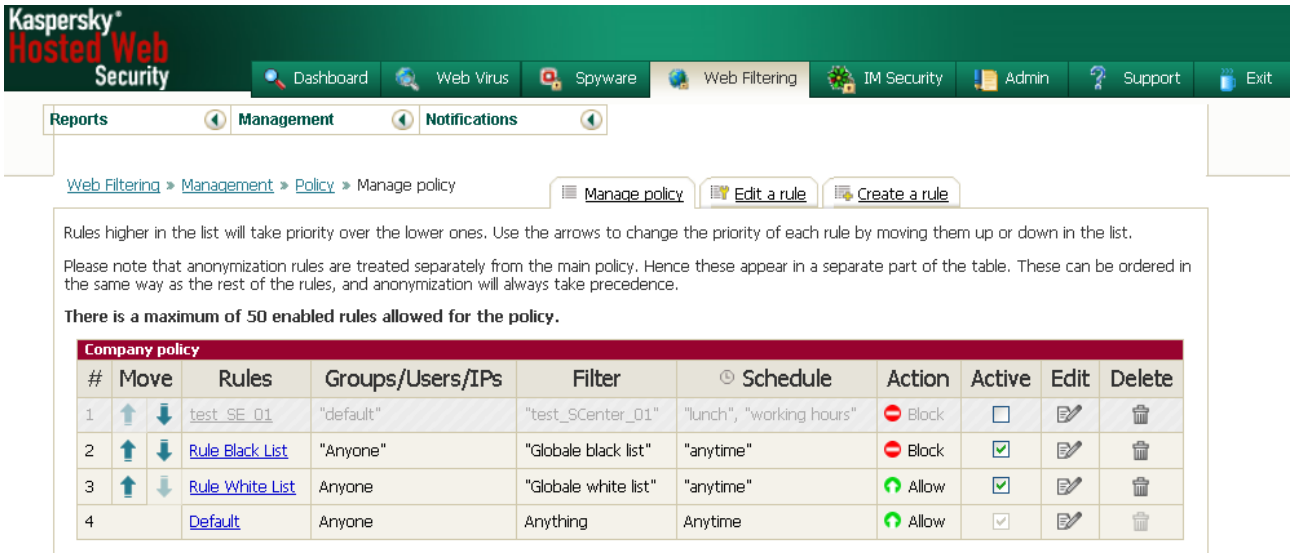


Once these filters have been created, you need to create two new rules in the policy.

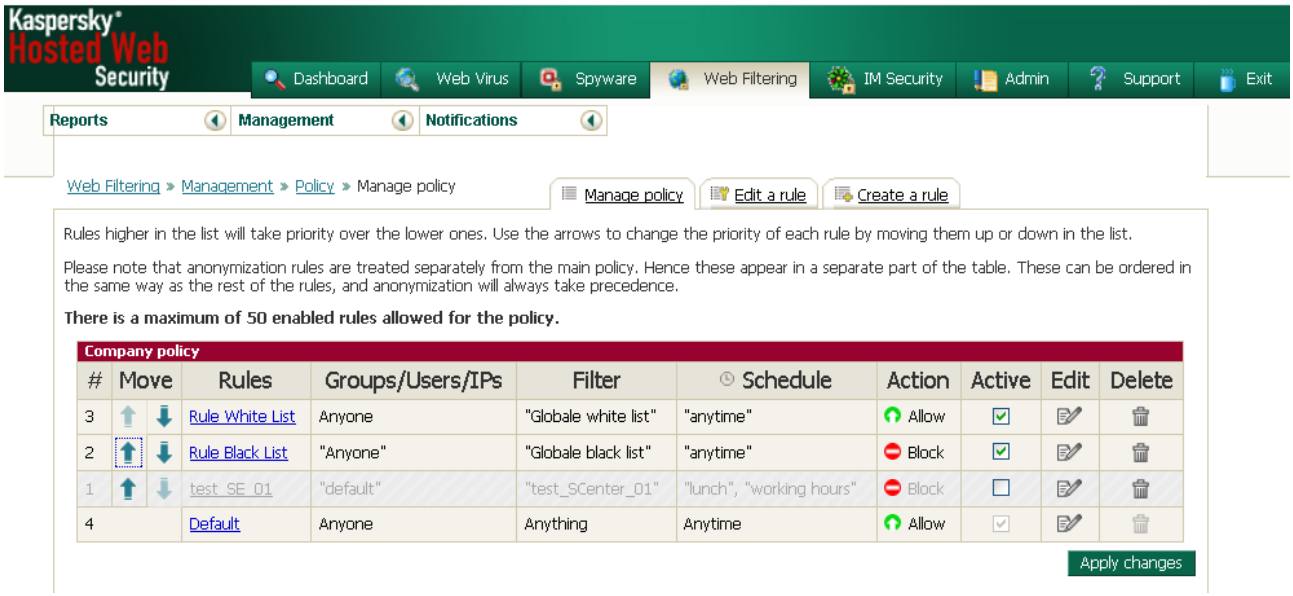
To create the Global White List rule, you should add the Global White List filter only to a rule called 'Global White List'.


Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Web Filtering » Management » Policy » Create a rule
Manage policy
Edit a rule
Create a rule
Rule name: Default
Name Default
Rule Action Allow
Define Group ("WHO")
Search for a group by clicking on "Add group". To set a group as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).
If no group is selected, this rule will apply to anyone. Adding multiple groups has the action of "OR", so users will need to be in any of the groups listed for the rule to take effect.
Group
Set as an exception
Delete
No group selected
Add group
Define Filters ("WHAT")
Choose a Filter from the list and click "Add". To set a Filter as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).
Adding multiple filters has the action of "AND", so each filter will need to match for the rule to take effect.
Add Filter
Choose a filter from the list
Add
Filter
Set as an exception
Delete
No filter selected
Define Schedule ("WHEN")
Choose a Schedule from the list and click "Add". To set a Schedule as an exception to the rule, select the corresponding "Set as exception" box (action of NOT).
Adding multiple schedule is not recommended unless one is going to be "Set as exception" (action of "AND NOT")
Add Schedule
Choose a schedule from the list
Add
Schedule
Set as an exception
Delete
No schedule selected
Reset
Save

To create the Global Black List rule you should add the Global Black List filter only to a rule called 'Global Black List'.


Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Web Filtering » Management » Policy » Manage policy
Manage policy
Edit a rule
Create a rule
Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.
Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.
There is a maximum of 50 enabled rules allowed for the policy.
Company policy
Move Rules Groups/Users/IPs Filter Schedule Action Active Edit Delete
1 test_SE_01 "default" "test_SCenter_01" "lunch", "working hours" Block
2 Rule Black List "Anyone" "Globale black list" "anytime" Block
3 Rule White List Anyone "Globale white list" "anytime" Allow
4 Default Anyone Anything Anytime Allow

These rules now need to be positioned correctly and activated. They will appear in the Company Policy list (inactive) just above the default rule.


Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Reports
Management
Notifications
Web Filtering » Management » Policy » Manage policy
Manage policy
Edit a rule
Create a rule
Rules higher in the list will take priority over the lower ones. Use the arrows to change the priority of each rule by moving them up or down in the list.
Please note that anonymization rules are treated separately from the main policy. Hence these appear in a separate part of the table. These can be ordered in the same way as the rest of the rules, and anonymization will always take precedence.
There is a maximum of 50 enabled rules allowed for the policy.
Company policy
Move Rules Groups/Users/IPs Filter Schedule Action Active Edit Delete
3 Rule White List Anyone "Globale white list" "anytime" Allow
2 Rule Black List "Anyone" "Globale black list" "anytime" Block
1 test_SE_01 "default" "test_SCenter_01" "lunch", "working hours" Block
4 Default Anyone Anything Anytime Allow
Apply changes

The Global White list should be moved to the top of the rules and the Global Black list should be just under it. Both rules should be activated.

QUOTAS

Quotas are only available when using the Connector.

Quotas enable you to limit the amount of Web access a user can have on a daily or weekly basis. There are four different ways by which you can control the access allowance for a user:

Period	Time period to apply quota policy to
Bytes In	Amount downloaded in Megabytes or Gigabytes
Bytes Out	Amount uploaded in Megabytes or Gigabytes
Time	Amount of time spent browsing in Minutes or Hours
Connections	Amount of connections made to the Web

When creating a quota, you can specify amounts for any combination of the access allowance types listed above. For example, you may wish to specify 'Bytes In' and 'Time' allowances only, in which case you would select amounts for these two parameters and leave the other two set to 'Unlimited'. If you have more than one allowance type set in a quota, then as soon as one of the allowance limits is reached, all further Web browsing will be blocked until the quota period expires.

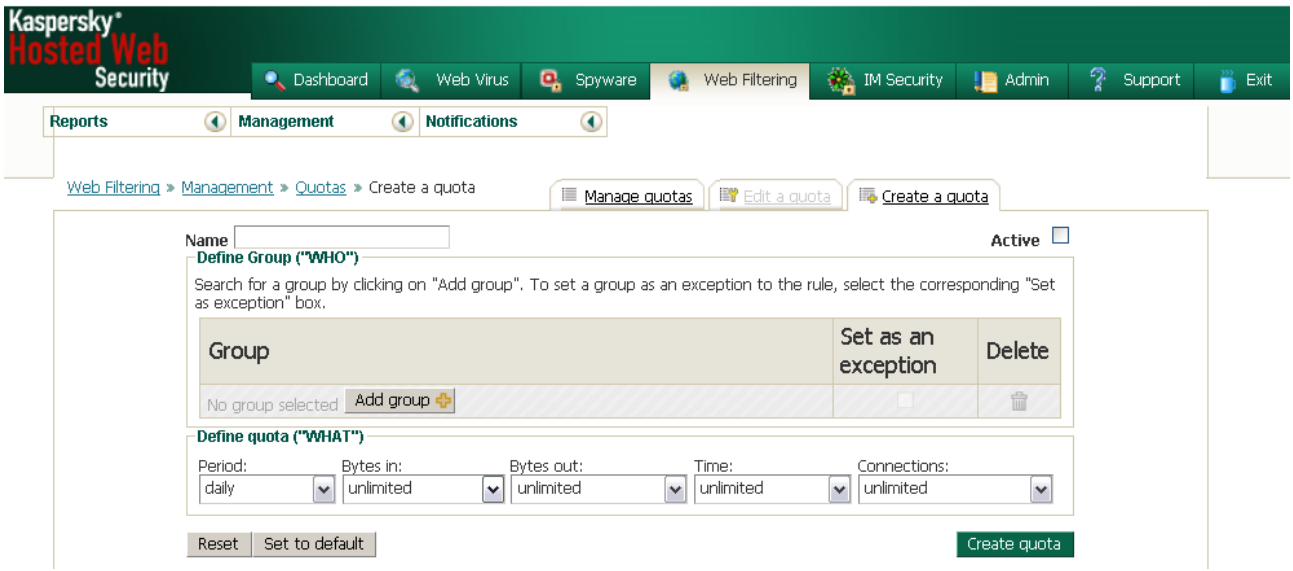
CREATING A QUOTA

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.

2. Under the Management sub-service dropdown, click the 'Quota'. This will bring up the 'Manage Quotas' screen.

3. Click the 'Create a Quota' tab. You will then be presented with a screen in which you can enter the configuration for the new Quota.

4. Enter a name for the new Quota into the provided text field.



5. Select the group to which you want to apply the Quota. (If you want this Quota to apply to everyone, then leave the group blank). By clicking the 'Browse' button you will see the group search selector. This selector will allow you to find a specific group (both custom and directory) from your list of groups. Click the 'Select' button next to the group and then click the 'Confirm Selection' button. The selector allows you to search for a group name (or part of), and you can also click a letter to choose all groups beginning with that letter. Once back to the 'Create a quota' screen, you will need to click the 'Add' button to add this to the Quota rule.

6. From the 'Period' drop down box, select the period of time in respect of which you would like the quota to apply (Daily or Weekly).

7. Select the limits you would like to set for 'Bytes in', 'Bytes Out', 'Time' and 'Connections', by choosing an amount from their corresponding drop down boxes.

If you do not wish to set a limit for a particular allowance type, just leave it set to 'unlimited'. Clicking the 'Reset' button will return all settings to 'unlimited'.

8. Click the 'Save' button to save your new Quota.

EDITING A QUOTA

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.

2. Under the Management sub-service dropdown, click the 'Quota'. This will bring up the 'Manage Quotas' screen.

3. There are three ways to edit a Quota.

4. Click the name of the Quota in the rules list.

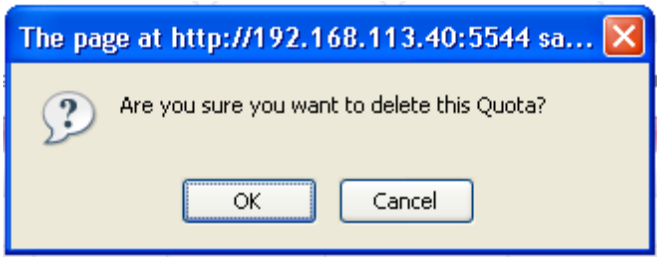
5. Click the edit button in the same row as the quota you want to edit.

6. Click the 'Edit a Quota' tab and select the quota rule from the dropdown.

7. The window will switch to the 'Edit a Quota' tab. You may then proceed to make any configuration changes to the Quota. Click the 'Save' button to save the modified Quota.

DELETING A QUOTA

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.
2. Under the Management sub-service dropdown, click the 'Quota'. This will bring up the 'Manage Quotas' screen.
3. Click the 'Delete' button corresponding to the quota you wish to delete. The following popup message will appear:



4. Click OK to delete the quota.
5. The page will refresh, and quota will no longer be shown in the list of existing quotas.

It is possible to inactivate a quota instead of deleting it. To do this, remove the tick from the active column in the Quota list, and click the apply changes button.

Возможно отключить квоту вместо ее удаления. Для этого снимите флажок в столбце Активно в списке квот и нажмите кнопку Применить изменения.

Можливо відключити квоту замість її видалення. Для цього зніміть прапорець в стовпці Активно в списку квот і натисніть кнопку Застосувати зміни.

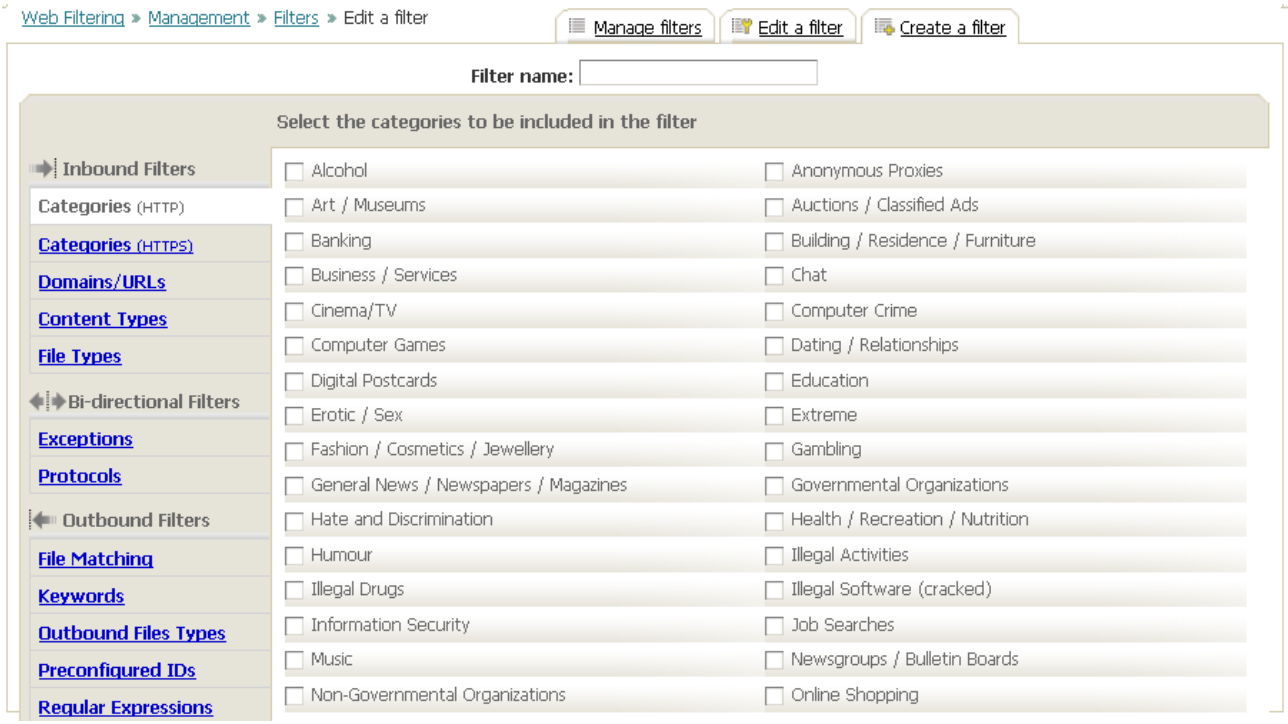
Możliwe jest wyłączenie limitu zamiast jego usunięcia. Aby to zrobić, usuń zaznaczenie w kolumnie Aktywny na liście limitów i kliknij przycisk Zastosuj zmiany.

Можно отключить квоту вместо ее удаления. Для этого снимите флажок в столбце Активно в списке квот и нажмите кнопку Применить изменения

SEPARATE HTTP/HTTPS FILTERING

By enabling this check box, the Filters page will alter to show two different tabs.

Clicking the Categories (HTTP) tab will take you to the page to define the restrictions for HTTP only traffic.



Clicking the Categories (HTTPS) tab will take you to the page to define the restrictions for HTTPS only traffic.

Should you choose at a later date to disable the separate HTTP/HTTPS filtering, the system will default back to the HTTP restrictions for both HTTP and HTTPS websites.

SEARCHAHEAD

Most users' Web-searching habits are based around a small number of set websites which they frequently visit, plus a search engine to find links to requested information. It is often during these searches that users can visit inappropriate and/or dangerous websites.

The Search*Ahead* option within Web filtering will annotate the Web searches within the supported search engines, so that users can tell in advance whether they should click the link or not. This advice is offered to end-users to stop them clicking links that may raise block events, and to stop them visiting websites that are known to harbor malware.

SUPPORTED SEARCH ENGINES

Google

www.google.com , www.google.co.uk , www.google.ca , www.google.de , www.google.com.au , www.google.ie , www.google.ru , www.google.dk , www.google.no , www.google.se , www.google.fi , www.google.nl

Yahoo

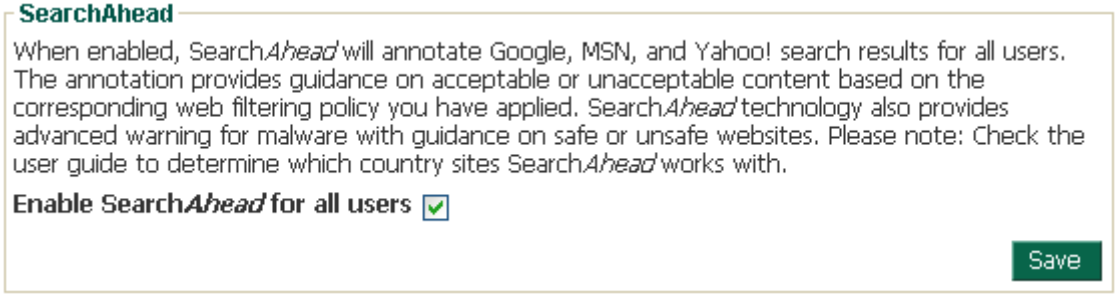
www.yahoo.com , www.yahoo.co.uk , www.yahoo.com.au , www.yahoo.ca , www.yahoo.ie , www.yahoo.dk , www.yahoo.no , www.yahoo.se , www.yahoo.fi

MSN

www.msn.com , www.msn.co.uk , www.msn.com.au , www.msn.ca , www.msn.ie , www.msn.de

STEPS NEEDED TO ACTIVATE SEARCHAHEAD FOR YOUR USERS

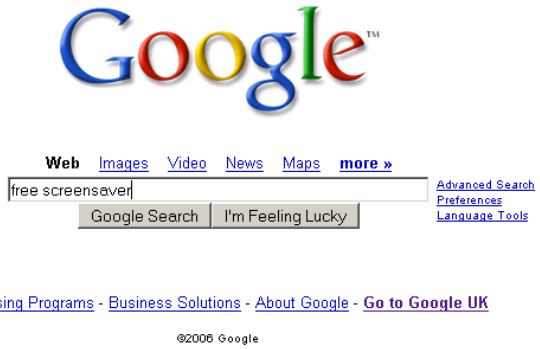
1. Click the 'Web Filtering' tab on the main navigation bar at the top of the screen.
2. Click the 'Global Settings' link in the 'Management' sub-service tab.


SearchAhead
When enabled, SearchAhead will annotate Google, MSN, and Yahoo! search results for all users. The annotation provides guidance on acceptable or unacceptable content based on the corresponding web filtering policy you have applied. SearchAhead technology also provides advanced warning for malware with guidance on safe or unsafe websites. Please note: Check the user guide to determine which country sites SearchAhead works with.
Enable SearchAhead for all users
Save

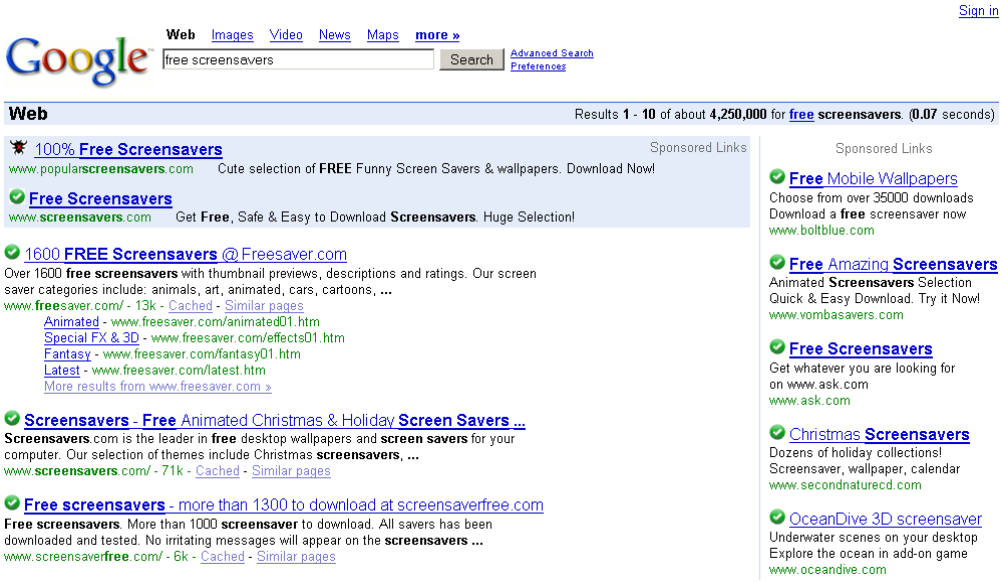
The Search*Ahead* option is a global setting for the company and cannot currently be deployed by group. Click the check box and click the 'Save' button to enable the Search*Ahead* function.

CHANGES TO THE SEARCH ENGINE SCREENS

End users can perform searches in exactly the same way as they currently do (including advanced searches).



Now each search result/advertising link will be annotated with an icon that displays information about the link based upon your corporate Web filtering policy and sites that contain malware.


Sign in
Google
Web Images Video News Maps more »
free screensavers
Search
Advanced Search
Preferences
Web
Results 1 - 10 of about 4,250,000 for free screensavers. (0.07 seconds)
100% Free Screensavers
Sponsored Links
www.popularscreensavers.com Cute selection of FREE Funny Screen Savers & wallpapers. Download Now!
Free Screensavers
www.screensavers.com Get Free, Safe & Easy to Download Screensavers. Huge Selection!
1600 FREE Screensavers @ Freesaver.com
Over 1600 free screensavers with thumbnail previews, descriptions and ratings. Our screen saver categories include: animals, art, animated, cars, cartoons, ...
www.freesaver.com/ - 13k - Cached - Similar pages
Animated - www.freesaver.com/animated01.htm
Special FX & 3D - www.freesaver.com/effects01.htm
Fantasy - www.freesaver.com/fantasy01.htm
Latest - www.freesaver.com/latest.htm
More results from www.freesaver.com »
Screensavers - Free Animated Christmas & Holiday Screen Savers ...
Screensavers.com is the leader in free desktop wallpapers and screen savers for your computer. Our selection of themes include Christmas screensavers, ...
www.screensavers.com/ - 71k - Cached - Similar pages
Free screensavers - more than 1300 to download at screensaverfree.com
Free screensavers. More than 1000 screensaver to download. All savers has been downloaded and tested. No irritating messages will appear on the screensavers ...
www.screensaverfree.com/ - 6k - Cached - Similar pages
Sponsored Links
Free Mobile Wallpapers
Choose from over 35000 downloads Download a free screensaver now
www.boltblue.com
Free Amazing Screensavers
Animated Screensavers Selection Quick & Easy Download. Try it Now!
www.vombasavers.com
Free Screensavers
Get whatever you are looking for on www.ask.com
www.ask.com
Christmas Screensavers
Dozens of holiday collections! Screensaver, wallpaper, calendar
www.secondnaturecd.com
OceanDive 3D screensaver
Underwater scenes on your desktop Explore the ocean in add-on game
www.oceandive.com

ANNOTATIONS

	This site is compliant with the Web usage policy set by your administrator.
	While this content is not blocked by your administrator, it is advisable to proceed with caution. (This will be seen if the category is covered by the 'Warn' action within the policy for the user.
	By clicking this link, you will be violating the Web usage policy set by your administrator.
	Use caution. This site may represent a potential Web risk (such as spyware, adware, viruses or phishing).

The following categories will have the orange icon displayed even if they are not blocked/warned by your organization:

- Illegal Activities
- Illegal Software
- Illegal Drugs
- Pornography
- Hate and Discrimination
- Extreme
- Erotic/Sex
- Unclassified

THE SEARCHAHEAD BUBBLE

By placing the mouse over the annotation, more detailed information is shown to the end-user.

The Search*Ahead* Bubble details whether or not the link is considered safe and passes your corporate Web Filtering policy. It will also show you the categorization for the site as well. Sites which fail the corporate Web Filtering policy clearly show this by the use of the Red Cross icon. Users will still be blocked from visiting the website in question if they click the link, but this should put an end to the majority of accidental clicks to inappropriate websites.

SearchAhead Results: Powered by ScanSafe
Screensavers - Free Animated Christma...
http://www.screensavers.com
This site is compliant with the web usage policy set by your administrator for the following reason:
Site Content: Software and
Distributors
ScanSafe SearchAhead
100% Free Screensavers
SearchAhead Results: Powered by ScanSafe
100% Free Screensavers
http://www.popularscreensavers.com
Use Caution. This site may contain a web risk such
Viruses or Phishing.
ScanSafe SearchAhead
Tobacco.org : Welcome
SearchAhead Results: Powered by ScanSafe
Tobacco.org : Welcome
http://www.tobacco.org
By clicking on this link you will be violating the web usage policy set by your administrator.
Site Content: Tobacco
ScanSafe SearchAhead

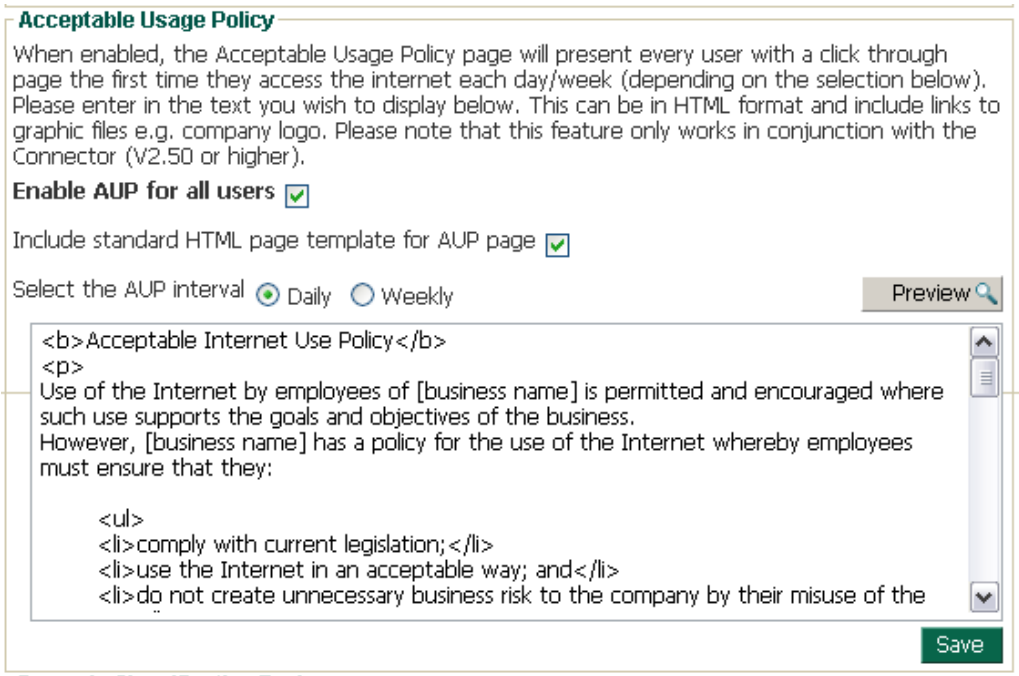
ACCEPTABLE USAGE POLICY SCREEN

Many users today claim to not be aware of the company's Acceptable Usage Policy (AUP) for the Web. To help our customers, Kaspersky Hosted Security provides a click-through Acceptable Usage Policy screen.

This parameter is available to customers using the Connector v2.5 or higher in conjunction with the SNMP, находятся в конфигурационном файле *snmp_settings*.

To enable this screen, do the following:

1. Click the Web Filtering tab.
2. Click the Global Settings option on the management menu. The screen opposite will appear.
3. To enable the AUP page, select the 'Enable AUP for all users' check box.


Acceptable Usage Policy
When enabled, the Acceptable Usage Policy page will present every user with a click through page the first time they access the internet each day/week (depending on the selection below). Please enter in the text you wish to display below. This can be in HTML format and include links to graphic files e.g. company logo. Please note that this feature only works in conjunction with the Connector (V2.50 or higher).
Enable AUP for all users
Include standard HTML page template for AUP page
Select the AUP interval
Daily
Weekly
Preview
Acceptable Internet Use Policy
<p>
Use of the Internet by employees of [business name] is permitted and encouraged where such use supports the goals and objectives of the business.
However, [business name] has a policy for the use of the Internet whereby employees must ensure that they:

comply with current legislation;
use the Internet in an acceptable way; and
do not create unnecessary business risk to the company by their misuse of the
Save

Kaspersky Hosted Security provides a sample AUP page to use as a template if your organization currently does not have one; however we recommend you seek professional advice in creating your own. Care should be taken to include references to the latest Web 2.0 technologies. If you are locking down your end-user laptops to only use the Internet through the Web Security services (both internally and externally), any means to circumvent this should be strictly prohibited in the AUP.

All AUP pages will have an 'I Agree' button at the bottom of the page for users to click. You should include in your AUP a statement that by clicking the 'I Agree' button the user agrees to abide by your AUP.

You have a choice as to how often the AUP page is displayed to the end user, namely either daily or once per week. Select the appropriate radio button which meets your requirements.

Kaspersky Hosted Security allows for fully customizable AUP pages, which means that you can define the entire HTML output of the block page up to and including the opening and closing <html> tags. This allows you to customize AUP pages with your own logo and policy text on the AUP page.

4. Uncheck the 'Include standard HTML page template for AUP page' box to remove the standard logo and default text from the AUP page.
5. Enter the desired HTML into the 'AUP' field. Any images/css referenced needs to be a resolvable location. Typically you will be required to host your own images/css for this page.

6. Once you are happy with the AUP Page modifications you have made, click the 'Save' button located at the bottom of the screen.

7. Click the preview button just beneath the text area to see how the additional information is rendered. You must save your changes before preview displays your new settings.

The AUP screens are only one of the many functionalities of the Kaspersky Anti-Virus Connector for Standalone SNMP. If the connector is reset, the end users will be required to read and accept the AUP screens will be displayed again to the end users.

FILTERING NOTIFICATIONS

Under the 'Filtering Notifications' sub-service tab, there are two settings which require configuration:

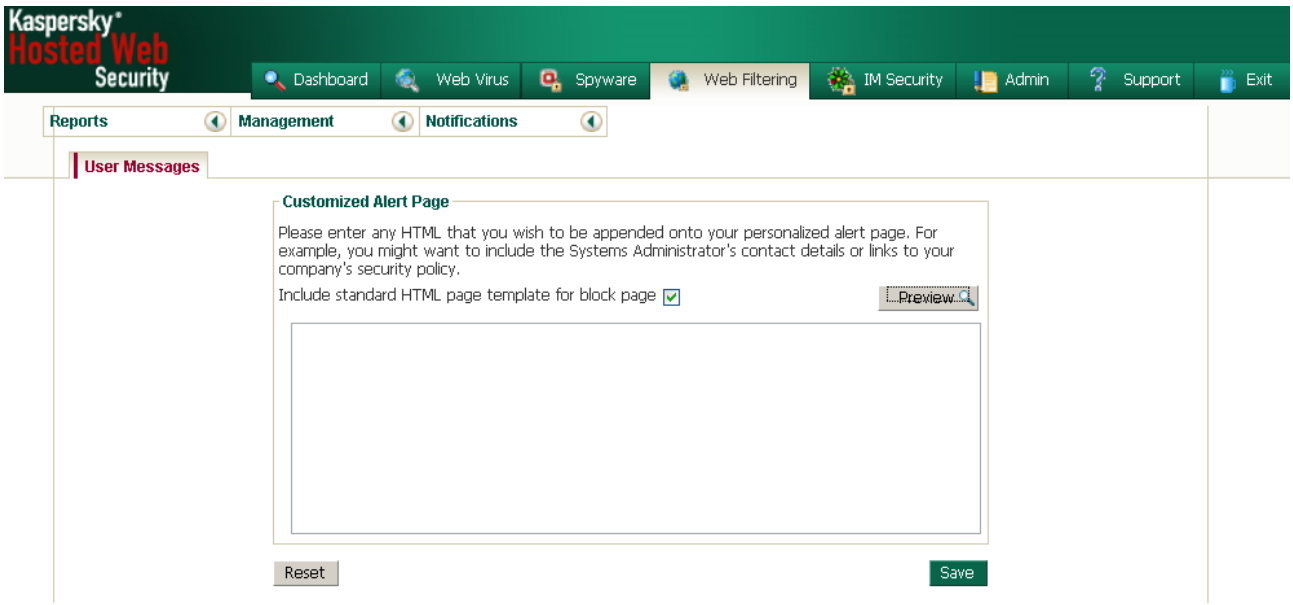
- **User Messages**: this allows you to specify the message which an end-user will see when a request is blocked.
- **Email Alerts**: this enables an administrator to receive an email alert for any blocked activity.

Further information is given on these settings below.

FILTERING USER MESSAGES

Kaspersky Hosted Security has two User Messages which are pages that your users will see in their Web browser if a URL they request is blocked or a warning page is displayed. In order to customize it for your organization, you can append your own information and add your company logo to the Default Alert Pages. For example, you may wish to add the System Administrator's contact details, or links to your organization's security policy.

Параметры управления работой Антивируса Касперского с мастер-агентом SNMP, находятся в конфигурационном файле *snmp_settings*.



Kaspersky Hosted Security allows for fully customizable block pages, which means that you can define the entire HTML output of the block page up to and including the opening and closing <html> tags. This allows you to customize block pages with your own logo and text on the block page.

1. Click the 'Web Filtering' service tab at the top of the screen.

2. Click the 'User Messages' button in the Notifications sub-menu. This will bring up the 'User Messages' screen. This has two sections, one for the Block page and one for the Warning page.

3. Uncheck the 'Include Kaspersky Lab headers' box to remove the Kaspersky Lab logo from the block page.

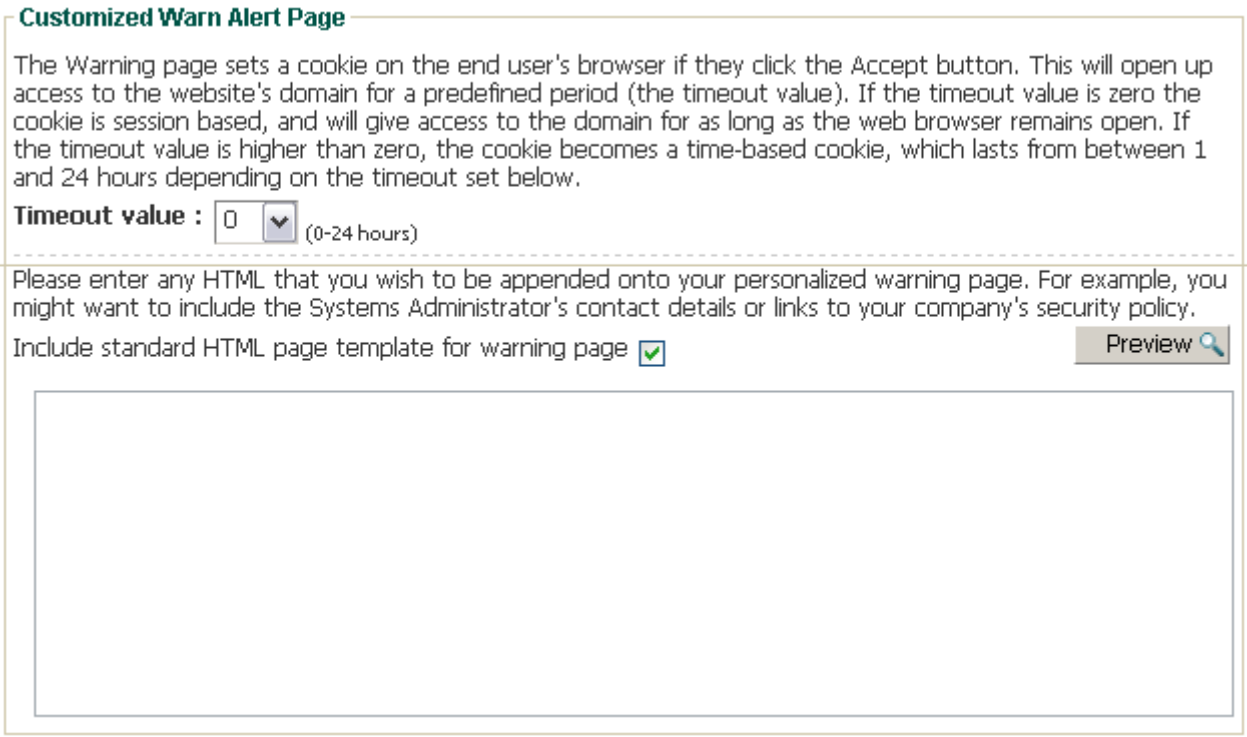
4. Enter the desired HTML into the 'User Messages' field. Any images/css referenced needs to be a resolvable location. Typically you will be required to host your own images/css for this page.

5. You may insert #reason, #url, #category or #username into the HTML and it will be parsed as the reason for the block event. More detail on this is available in the next section.

6. Once you are happy with the Alert Page modifications you have made, click the 'Save' button located at the bottom of the screen.

7. Click the 'Preview' button just beneath the text area to see how the additional information is rendered. You must save your changes before your new settings can be previewed.

8. The Warning page has an extra setting for the timeout value of the cookie which is set for the domain when the end user accepts the warning page. If the timeout value is set to zero, the cookie becomes session-based, and will give access to the domain for as long as the web browser remains open. If the timeout value is higher than zero, the cookie becomes a time-based cookie, which lasts between 1 and 24 hours depends on the value set. On subsequent visits to the same domain, the cookie will be checked and if still valid the user will be allowed to access this website. Please note that this a global value for all WARN pages. Please also note that the Warn functionality only works on HTTP websites at this time; HTTPS websites will be processed by the policy as normal, and will fall through depending on the subsequent actions in the rules.


Customized Warn Alert Page
The Warning page sets a cookie on the end user's browser if they click the Accept button. This will open up access to the website's domain for a predefined period (the timeout value). If the timeout value is zero the cookie is session based, and will give access to the domain for as long as the web browser remains open. If the timeout value is higher than zero, the cookie becomes a time-based cookie, which lasts from between 1 and 24 hours depending on the timeout set below.
Timeout value :
0
(0-24 hours)
Please enter any HTML that you wish to be appended onto your personalized warning page. For example, you might want to include the Systems Administrator's contact details or links to your company's security policy.
Include standard HTML page template for warning page
Preview

USING VARIABLES TO CUSTOMIZE BLOCK PAGE TEXT

You may insert #reason, #url, #category or #username into the HTML in your custom block page and the block page will show the reason for the block event. An example to the right shows this more clearly.

Default block message:

```
URL contained in custom redlist default
Blocked Category : SMS / Ring Tones / Logos
EICAR-Test-File
```

Custom HTML message written by user:

```
<b>#reason<b><br>
#reason is not allowed by acme corps
```

Custom message text will appear in end-user block page:

```
<b> EICAR-Test-File<b><br>
 EICAR-Test-File is not allowed by acme corps
```

FILTERING EMAIL ALERTS

The Filtering Email Alerts are emails that notify you of when Kaspersky Hosted Security has blocked a Web page. The email will contain the following information:

- The IP address from which the request left your organization.
- The Internal IP address and or the user/group (if available – requires installation of a Connector).
- The reason the requested page was blocked.
- The full URL of the requested page.

EMAIL GENERATION

1. Click the 'Web Filtering' service tab on the main navigation bar at the top of the screen.
2. Click the 'Email Alerts' link in the Notifications sub-service tab. This will bring up the 'Email Alerts' page.
3. Select whether or not you want to be notified when a Web page is blocked by selecting 'Yes' or 'No' from the drop down box.
4. Enter the email address (or addresses) you want notifications to be sent to in the empty text fields provided. You can specify a maximum of five different email addresses to which you wish to have these alerts sent. If you require the alerts to be sent to more addresses than this, we recommend that you set up a group mailing address.
5. If you wish to throttle the amount of email alerts you receive, click in the box next to the statement 'Limit these alerts to'. Throttling will now be activated and you must then select the number of alerts you wish to receive, per the amount of hours you specify. For example, you might decide that you only ever want to get a maximum of three email alerts in any two-hour period.
6. Once you are happy with the Email Alert details you have entered, click the 'Save' button located at the bottom of the screen.

IM CONTROL

The IM Control service enables you to:

- Configure, enforce, and monitor IM use within your organization.
- View comprehensive, filtering related information in the form of statistical reports, graphs, tables and exportable data files, based on your IM traffic and filtering blocks.
- Set up and manage email alerts for monitoring.

Changes made to IM Control settings will be applied to your live IM Control service within 60 seconds of submission via Kaspersky Hosted Security portal.

CONFIGURING DOMAINS FOR AUTHENTICATED USERS

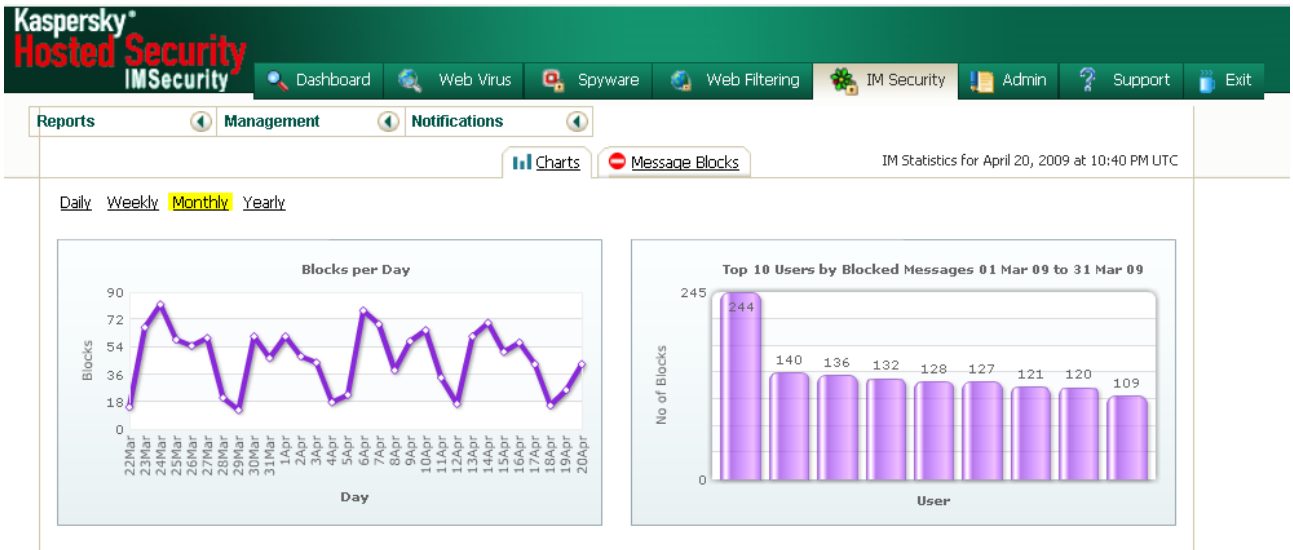
Users have their public IM address/handle matched up with their Network Identifier to ensure full accountability for all users. On the first use of an unrecognized screen name, the user is prompted to register, and taken to a Web page where they enter their company e-mail address. This is then authenticated by e-mail verification. Until this verification is completed, the user will not be able to use their IM address/handle.

Given that only certain domains will be used, and the need to ensure that users only enter their corporate e-mail address, you need to add the corporate domains(s) to be used before implementing the IM Control service. Please contact KHSS-Support@kaspersky.com to request additional company domains.

IM CONTROL DASHBOARD

The dashboard gives you a live, 'at-a-glance' view of the filtering status. To access the dashboard, click 'IM Control' at the top of the screen and you will be presented with a filtering status summary.

The timescales for the data to be generated for viewing as a summary are the last day, week, month or year, and this can be selected by choosing the corresponding link above the graph.



Currently two graphs are available:

- **Blocks per period**: this shows the number of IM block events for the selected time period.

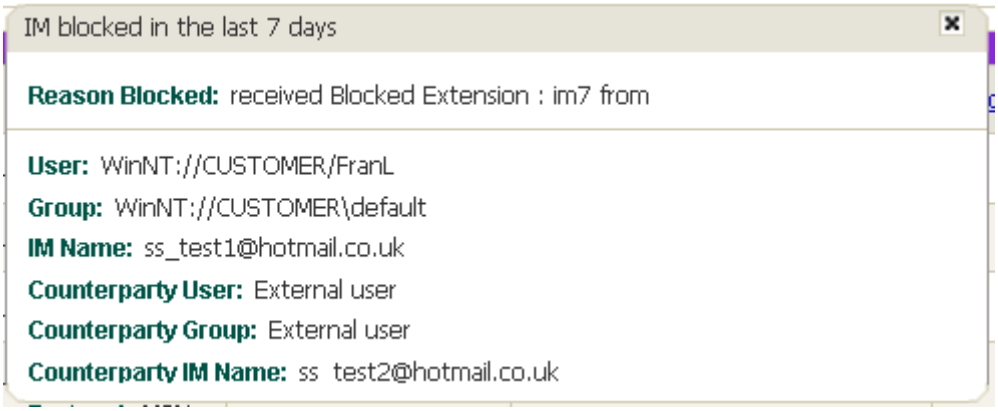
- Top 10 Users by Blocked Messages.

  This shows the following information: Date, User, Group, IM Name, Reason Blocked, Counterparty User, Counterparty Group, Counterparty IM Name, Protocol, Message Text.

It is also possible (in the second tab) to view all the IM filtering blocks for the given time period. The table shows 100 entries at a time and orders them by most recent. There are links at the bottom of the table to step back in lots of 100, until you reach the very first message block for the given time period. For each message blocked caught, the table will display:

- The date and time the message was blocked.
- The user from whom the blocked message originated.
- The screen name of the user from whom the blocked message originated.
- The reason it was blocked.
- The protocol through which the message was blocked.
- The message text that triggered the block.

By clicking the more info button you will see more information based on this block.


IM blocked in the last 7 days
Reason Blocked: received Blocked Extension : im7 from
User: WinNT://CUSTOMER/FranL
Group: WinNT://CUSTOMER\default
IM Name: ss_test1@hotmail.co.uk
Counterparty User: External user
Counterparty Group: External user
Counterparty IM Name: ss test2@hotmail.co.uk

IM CONTROL REPORTS

There are three different types of reporting available for IM Control:

- Summary Reports
- Scheduled Reports
- Forensic Audit Reports.

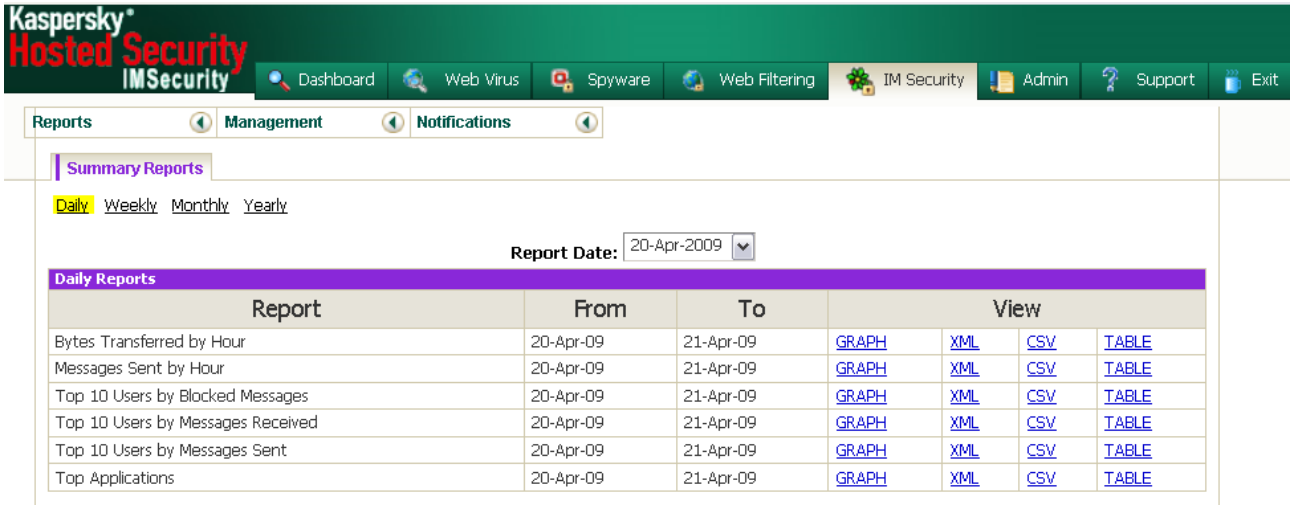
IM CONTROL SUMMARY REPORTS

This feature provides IM Control reporting, available either as a table, graph or exportable file. The exportable file allows for the import of the report data into another reporting application. This export data is available in two formats: CSV (Comma Separated Value) and XML (Extensible Mark-up Language). Kaspersky Hosted Security generates this report once a day from the IM traffic that your organization generates within a 24-hour period. The report comes in daily, weekly, monthly and yearly formats, allowing you to review all of the logged events which your organization has blocked. This information can be used to help formulate the type of access restrictions to apply within your organization and in modifying or fine-tuning your current restrictions.

VIEWING THE REPORTS

1. Click the 'IM Control' service tab at the top of the screen.

2. Click the 'Reports' link and select 'Summary Reports'.



3. Select the required reporting period from the top of the page (Daily, Weekly, Monthly or Yearly).

4. From the pull-down list, select an end date for the reporting period.

5. To view a specific report, simply click the 'Graph' button located just to the right of the report's name, underneath the 'View' heading. This will open up a separate window for displaying the graph.

6. If you wish to view a report in table format, simply click the 'Table' button instead. This will open up a separate window to display the table.

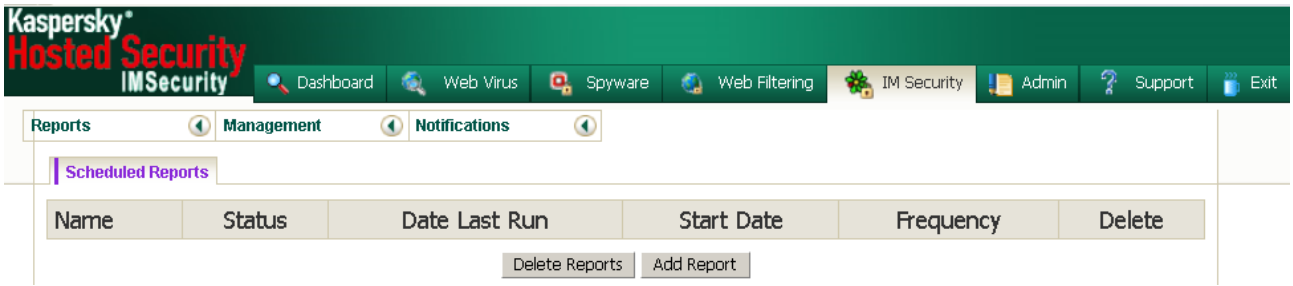
7. To download the report data in either CSV or XML format, simply click the 'CSV' or 'XML' buttons. You will then be prompted by your browser to specify a save location for the data file.

IM CONTROL SCHEDULED REPORTS

This feature provides IM Control scheduled reporting, available either as a table, graph or both. You can select the type of presentation, report date range, users to report on, the report generation scheduled, formatting options, and who to email the report to. Kaspersky Hosted Security generates this report once a day from the IM traffic that your organization generates over a 24-hour period.

EDIT AN EXISTING IM CONTROL SCHEDULED REPORT

1. Click the 'IM Control' service tab at the top of the screen.



2. Click the 'Reports' link and select 'Scheduled Reports'.

3. From the IM Control Scheduled Reports page, you can click available reports by clicking their name, which is underlined as a link, to edit the report.

4. The report will allow you to change all options, except that the presentations that were previously selected are not editable. If you wish to change the presentations you wish to report upon, you should create a new scheduled report.

5. Once you have finished editing the existing scheduled report, click the 'Update Report' button to save your changes.

DELETE AN EXISTING IM CONTROL SCHEDULED REPORT

1. Click the 'IM Control' service tab at the top of the screen.

2. Click the 'Reports' link and select 'Scheduled Reports'.

3. From the IM Control Scheduled Reports page, you can click the checkbox to the right of the available reports, and then click the 'Delete Reports' button to delete the selected reports. A validation message will appear to ask if you are sure you want to delete the selected reports. Click 'OK' to delete the reports.

ADD AN IM CONTROL SCHEDULED REPORT

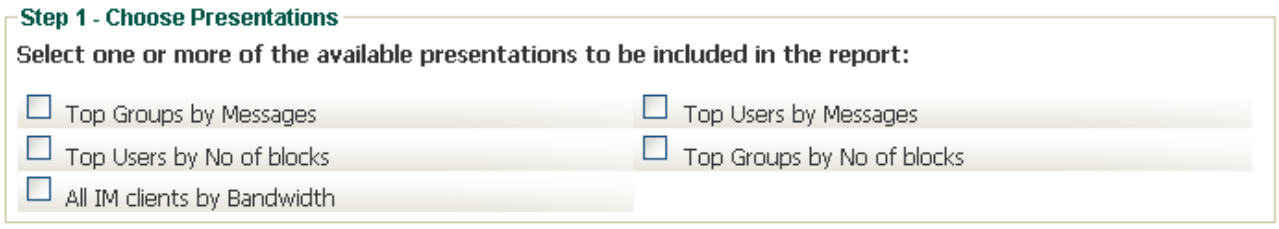
1. Click the 'IM Control' service tab at the top of the screen.

2. Click the 'Reports' link and select 'Scheduled Reports'.

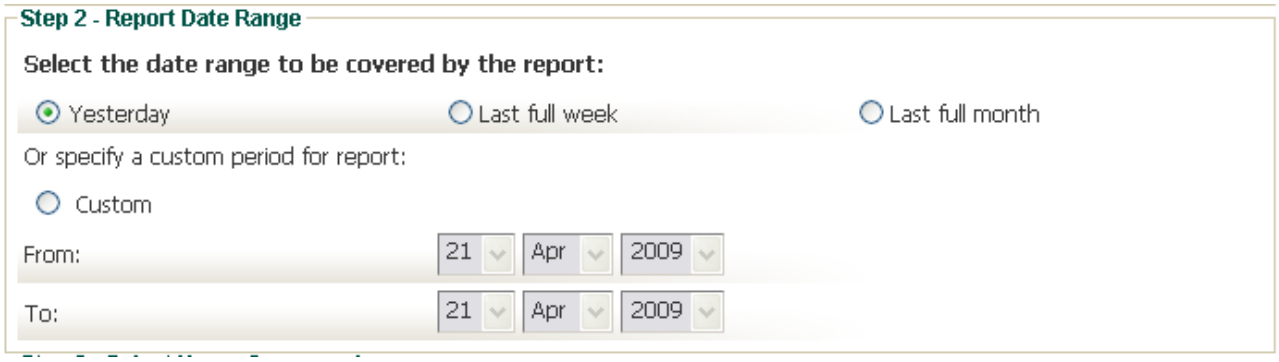
3. From the IM Control Scheduled Reports page:

   - **Step 1**: Select from the available presentations to be included in the report.

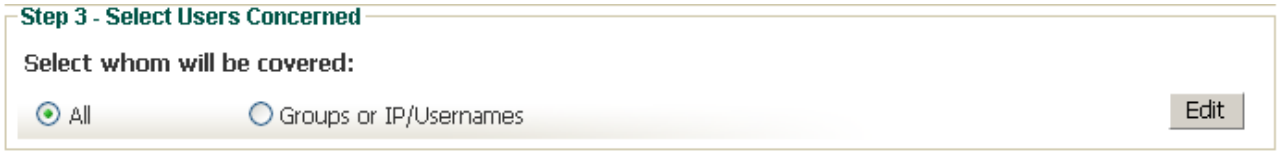
     - Top Users by Messages
     - Top Users by No of blocks
     - All IM clients by Bandwidth
     - Top Groups by Messages
     - Top Groups by No of blocks


Step 1 - Choose Presentations
Select one or more of the available presentations to be included in the report:
Top Groups by Messages
Top Users by Messages
Top Users by No of blocks
Top Groups by No of blocks
All IM clients by Bandwidth

- **Step 2**: Select the desired date range required either Yesterday, Last full week, Last full month or a customized date range.

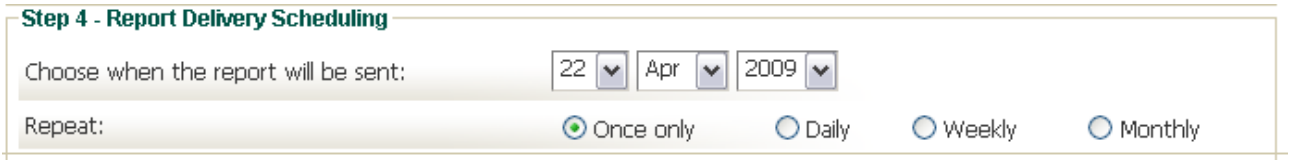


- **Step 3**: Select either all users or specific users or groups by clicking the 'Edit' button. The Groups and User IPs screen show the available groups and User or IP addresses that are available to be reported on. This data is based on the monitored traffic.

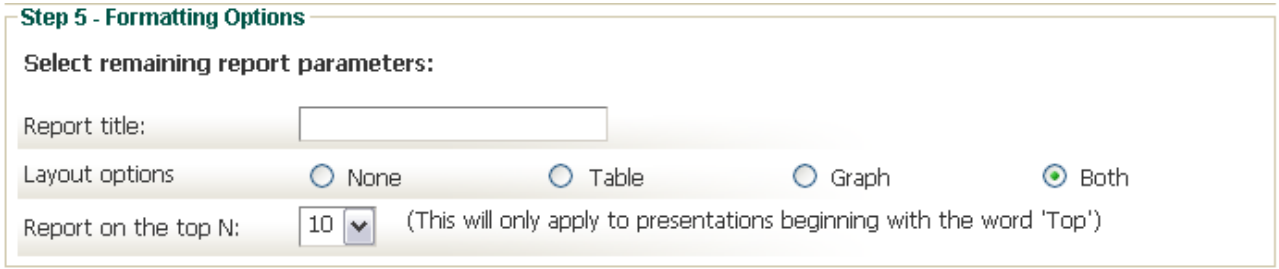


If the list is too long, you can search for a user by typing the information in the search box and the username, group name or IP address is highlighted in the list. When you have finished selecting specific groups or users, click 'Save' to go back to the previous screen.

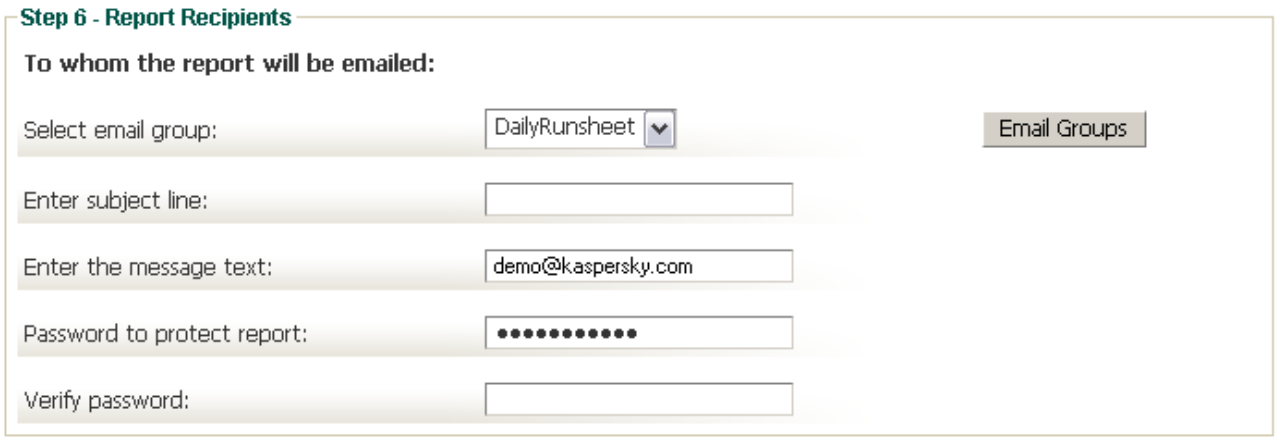
- **Step 4**: Schedule the report delivery, by selecting the specific start date using the drop down boxes, and selecting the frequency of the scheduled report delivery – either Once only, Daily, Weekly or Monthly.



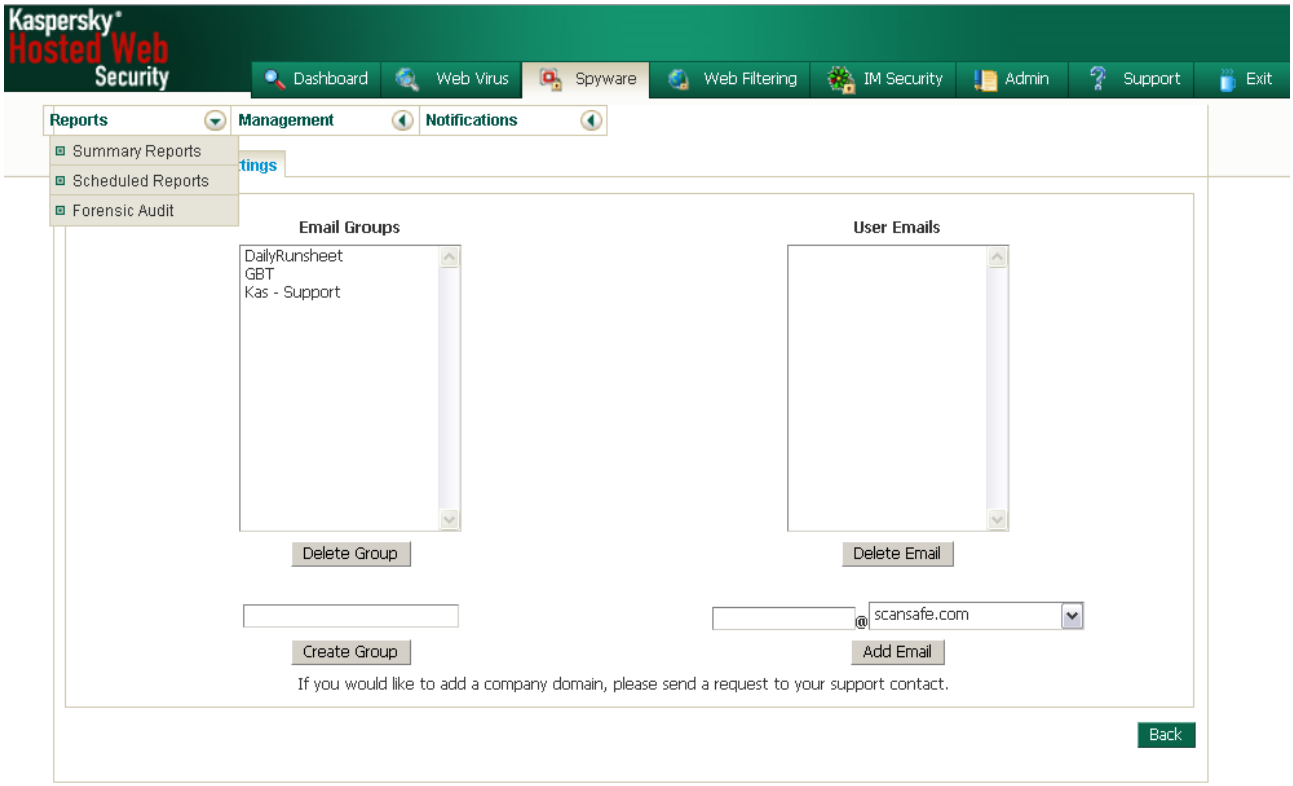
- **Step 5**: Select formatting options for the report (including typing in a report title) and layout options by selecting a table or graph presentation or both. You may also select the top 'N' (number) for the presentations you have selected, such as the 'Top 50 Viruses Blocked'.



- **Step 6**: Select the report recipients by selecting the email group, entering the subject line of the email, the message text and a password to open and review the report. If you want to create new email groups or edit existing ones, click the 'Email Groups' button.



Select the Email Group on the left side to see the email addresses assigned to that group on the right side. You can add new email groups, delete groups, and remove and add email addresses. Email addresses are restricted to the company domain that is created when your account is created. If you would like to add additional company domains, please contact KHSS-Support@kaspersky.com. Click the 'Back' button to return to the previous screen. Click the 'Activate Report' button when you have finished.



IM CONTROL FORENSIC AUDIT

The Forensic Audit sub-service enables an administrator to receive a detailed audit trail of all IM Control activity. The requested activity is then viewable as a CSV file.

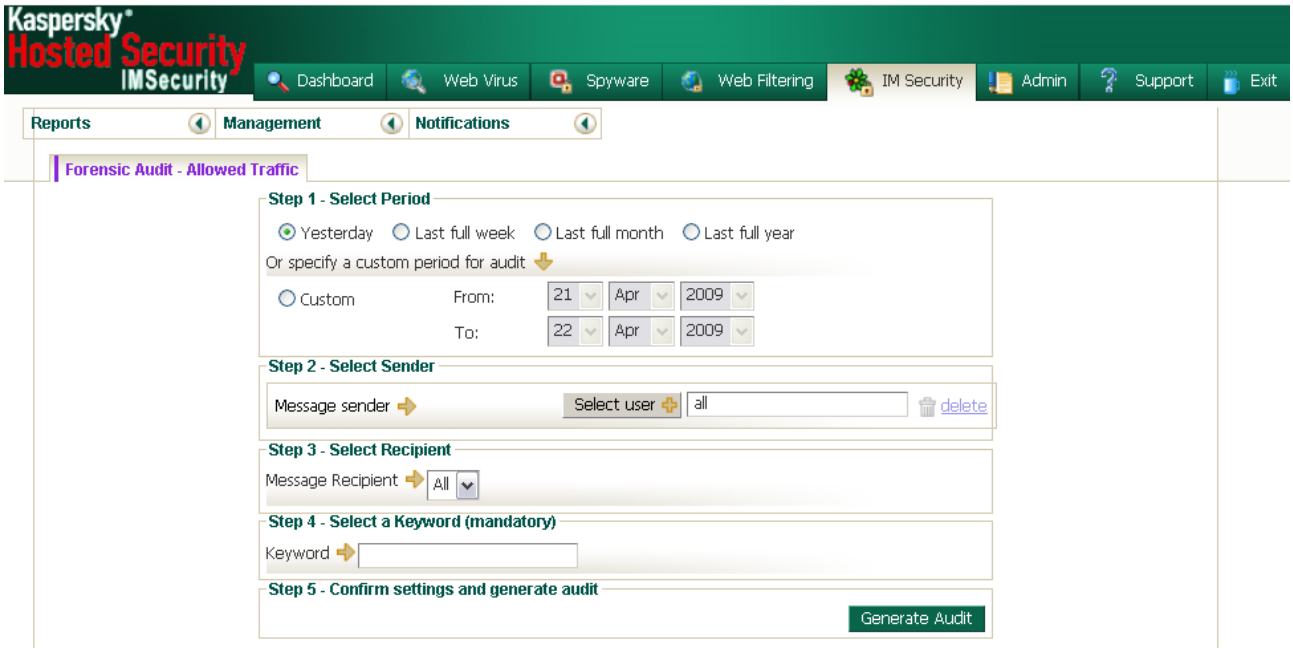
ALLOWED TRAFFIC

The IM Control Allowed Traffic sub-service enables an administrator to receive a detailed audit trail of all IM Control activity that contains a user-defined keyword.

➧ *To generate an IM Control Forensic Audit of Allowed Traffic:*

1. Click the 'IM Control' service tab at the top of the screen.

2. Click the 'Reports' link and select 'Forensic Audit – Allowed Traffic'.



3. From the Forensic Audit page, select the desired date range required: either Yesterday, Last full week, Last full month or a customized date range.

4. Select who the audit is about – this can mean a specific user or the entire company. (See 'User Selection Tool' on page 17 for more information).

5. Enter in a keyword for what you are looking for.

6. Click 'Generate Audit'.

7. From the pop-up, select 'Open' to immediately view the file in Excel, or select 'Save' to save the data in a CSV Excel file.

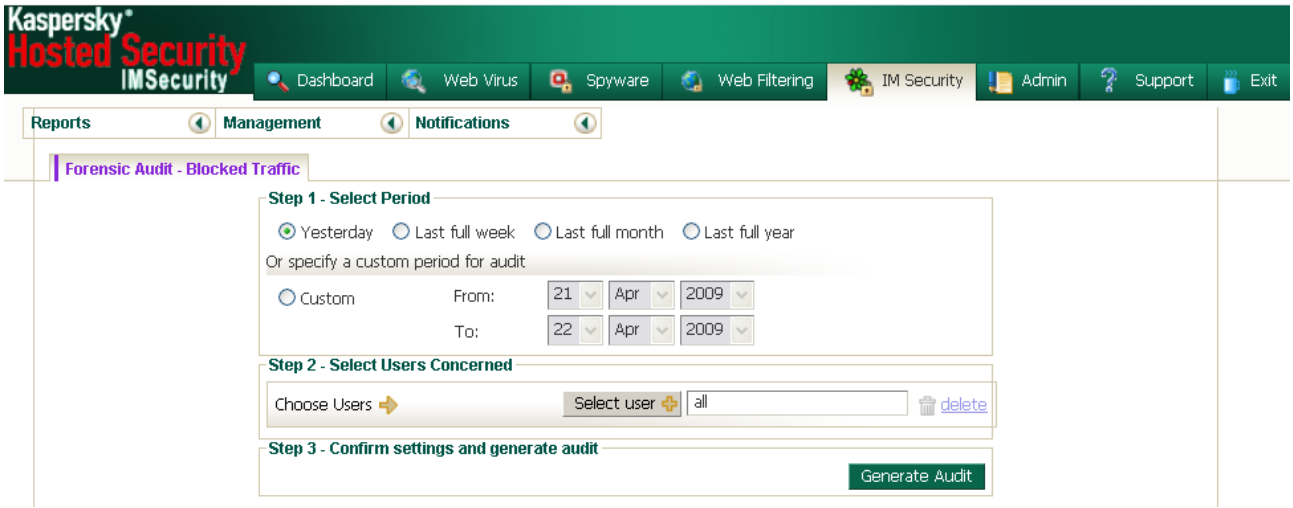
The requested activity is exported to a CSV file and contains the following data:

- **Date/Time**: date and time of the blocked message/file transfer.
- **Score**: the Kaspersky Hosted Security Relevance Engine evaluates the relevance of the keyword searched for to the messages identified.
- **Message**: the message that has been deemed as relevant according to the keyword entered.
- **Sending User**: the user who sent the message.
- **Receiving User**: the user who received the message.

BLOCKED TRAFFIC

The IM Control block traffic sub-service enables an administrator to receive a detailed audit trail of all IM Control activity resulting in a blocked request. The requested activity is exported to a CSV file and contains the following data:

- **Date/Time**: date and time of the blocked scan / event.
- **Threat Type**: lists the nature of the block.
- **User**: identifies the IP address of the customer site.
- **Group**: identifies the directory group where the request originated (if available – requires installation of the Connector).
- **Message**: the blocked message.



The report can be generated in a similar way to the 'Allowed Traffic' report (see 'Allowed Traffic' on page 75).

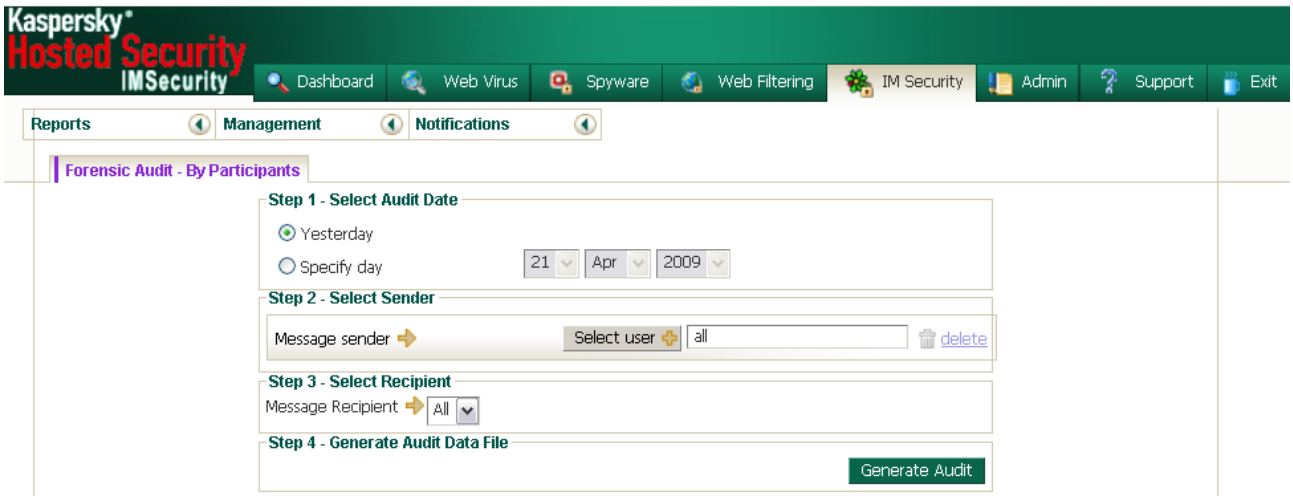
Date	Threat Type	User	Group	Message
09-Oct-2006 12:17:54 BST	im2	WinNT://CUSTOMER/AdamB	default	oh crikey
09-Oct-2006 12:19:51 BST	im2	WinNT://CUSTOMER/DonaldH	default	show me the money
09-Oct-2006 12:24:09 BST	im1	WinNT://CUSTOMER/AdamB	default	really secret data
09-Oct-2006 12:24:52 BST	im1	WinNT://CUSTOMER/HannahC	default	show me the money
09-Oct-2006 12:31:45 BST	im2	WinNT://CUSTOMER/AdamB	default	you are a very naughty boy
09-Oct-2006 08:15:14 BST	im4	WinNT://CUSTOMER/BenW	default	oh crikey
09-Oct-2006 09:17:59 BST	im4	WinNT://CUSTOMER/GeorgeP	default	david beckham
09-Oct-2006 09:28:50 BST	im5	WinNT://CUSTOMER/TomP	default	really secret data
09-Oct-2006 09:42:08 BST	im8	WinNT://CUSTOMER/AdamB	default	michael jackson

BY PARTICIPANTS

The IM Control 'By Participants' sub-service enables an administrator to receive a detailed audit trail of all IM Control activity that contains data between two participants. The requested activity is exported to a CSV file and contains the following data:

- **Date/Time**: date and time of the blocked scan / event.
- **Message**: the message.
- **Sending User**: the user who sent the message.
- **Receiving User**: the user who received the message.

The report can be generated in a similar way to the 'Allowed Traffic' report (see 'Allowed Traffic' on page 75).



IM MANAGEMENT

The process of configuring IM Control policy requires the use of several 'IM Control objects'. Each of these objects is listed in the left hand column under the IM Control Policy Manager sub-service. These objects are:

- **Groups**: a group is a collection of users who share similar access privileges. A group can be defined using directory information, such as directory group or username, or by network parameters such as IP address or subnet. For further details, see 'Group Management' on page 89.
- **Dictionaries**: these are where words to be blocked or alerts to be generated are specified. These are implemented in the Access Restrictions.
- **Access Restrictions**: each Access restriction consists of the following objects:

- Applications
- Dictionaries

Each of these objects is defined specifically for each Access Restriction.

- **Schedules:** a Schedule is a pre-defined period of time and days, based on a 7 day week and a 24 hour clock. They are defined globally, but can be assigned and 're-used' within any Policy.
- **Policies:** a Policy is a combination of a group (user or directory identity), schedule, and access restriction (IM Control access privileges – see 'Restrictions' on page 78).

DICTIONARIES. CONFIGURING THE DICTIONARIES

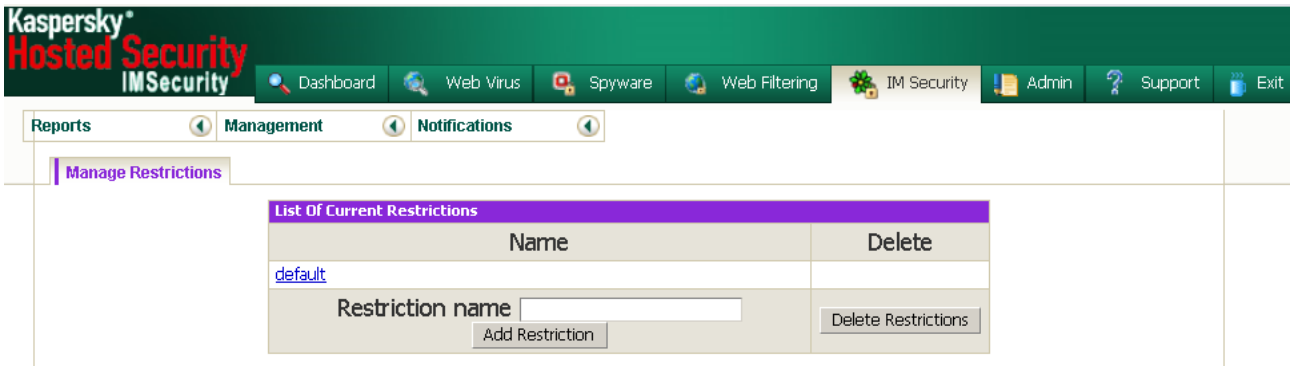
1. Click the button 'Dictionaries' from the 'Management' sub-service menu.
2. Create a new dictionary by entering the name of the new dictionary in the 'Add Dictionary' box. Then click the 'Add Dictionary' button.
3. Select the dictionary you want to edit, which takes you to the 'Language List' page. Enter the words or phrases one at a time, then click 'Add'. The word list will build in the text list beneath.
4. To delete words or phrases in the Language List, select the words and click 'Delete'.
5. Before leaving the page, click the 'Save' button to ensure all changes are registered.

RESTRICTIONS

In Kaspersky Hosted Security, a 'Restriction' is a set of user-defined IM Control rules. These IM Control rules are broken down into two different components:

- **Applications**: these relate to the IM client/platform that is to be allowed or blocked. In addition 'add-on' services such as video, gaming and chat can be blocked.
- **Dictionaries**: this specifies which word groups should be blocked from conversation or alerts generated. The dictionary content (i.e. the specific words to be blocked) needs to be stipulated in the Dictionary option in the Policies sub-service.

All external file transfers are blocked.



DEFAULT RESTRICTION

The 'Default' restriction is the restriction that will apply to any user that is not a member of a defined Group (either Custom Group or Directory Group). It is also the restriction that will apply to a Group that does not have a pairing with a Schedule that matches the current time. With this in mind, it is important to note that no users or Groups will ever be completely blocked from browsing. If there are no matching rules then the 'Default' restriction will always apply. **As a result, it is important that you take the time to configure the IM Control settings for the 'Default' restriction. Otherwise, whenever the restriction is in effect, full access will be given.**

The Default restriction can only be edited; it cannot be renamed or deleted.

CREATING A NEW RESTRICTION

1. Click the 'IM Control' service tab on the main navigation bar at the top of the screen.
2. Click the 'Management' sub-service tab and select the 'Restrictions' button.
3. The main 'Manage Restrictions' page presents you with a listing of all your current access restrictions.
4. To create a new restriction, enter the name of the new Restriction in the 'Please enter the new Restriction name' text field, then click 'Add Restriction'. You will then see your new restriction added to the 'List of current restrictions'.
5. The name of the new Restriction will now appear in the 'Manage Restrictions' page.

EDITING OR VIEWING A RESTRICTION

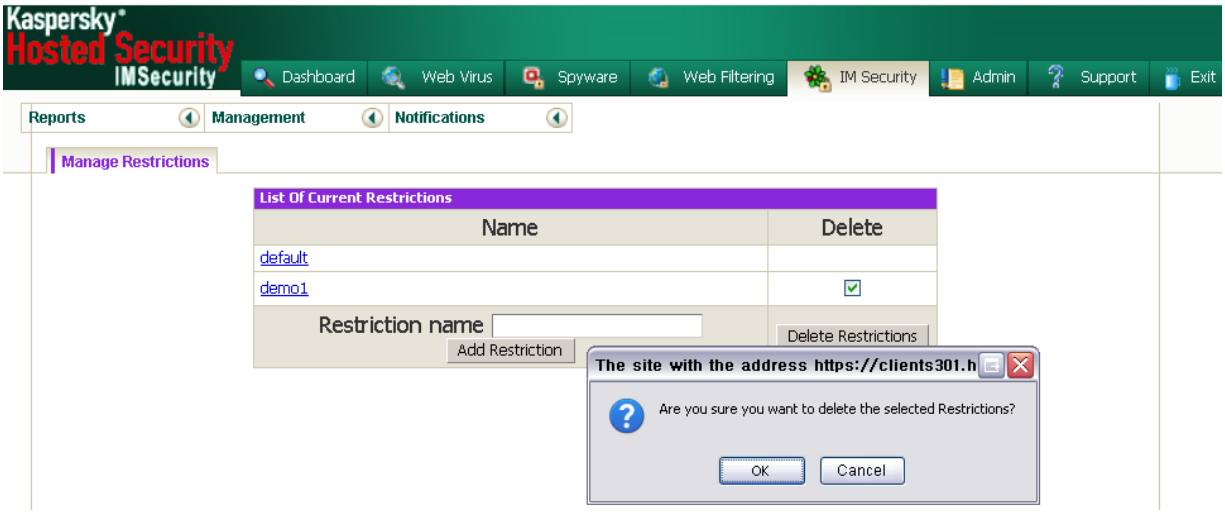
1. Click the 'IM Control' service tab on the main navigation bar at the top of the screen.
2. Click the 'Management' sub-service tab and select the 'Restrictions' button.
3. The main 'Manage Restrictions' page presents you with a listing of all your current restrictions. To review the settings for a particular restriction, click the corresponding restriction in question. The components of the requested Restriction (as detailed at the top of the page) will then appear.
4. You can now click 'define' for either or both of the components (Applications and Dictionaries). It is recommended that the administrator configure each component in series, starting at the top of the menu.
5. If no edits are required, hit the 'Back' button to return to the 'Manage Restrictions' listing.

DELETING A RESTRICTION

1. Click the 'IM Control' service tab on the main navigation bar at the top of the screen.
2. Click the 'Management' sub-service tab and select the 'Restrictions' button.
3. The main 'Manage Restrictions' page presents you with a listing of all your current restrictions. In order to delete one of these, click the checkbox corresponding to the existing restriction you wish to delete, and then click the 'Delete Restrictions' button located to the bottom right of the list of restrictions.

4. A dialog box will appear, asking if you are sure you want to delete the access restriction. Click the 'OK' button to proceed with deletion. The deleted restriction will no longer be displayed in the list on the main 'Manage Restrictions' page.

If the restriction you have chosen to delete has one or more pairings associated with it in the Policies listing Kaspersky Hosted Security will not let you delete it. You must first delete the dependent policy, followed by the restriction.



APPLICATIONS

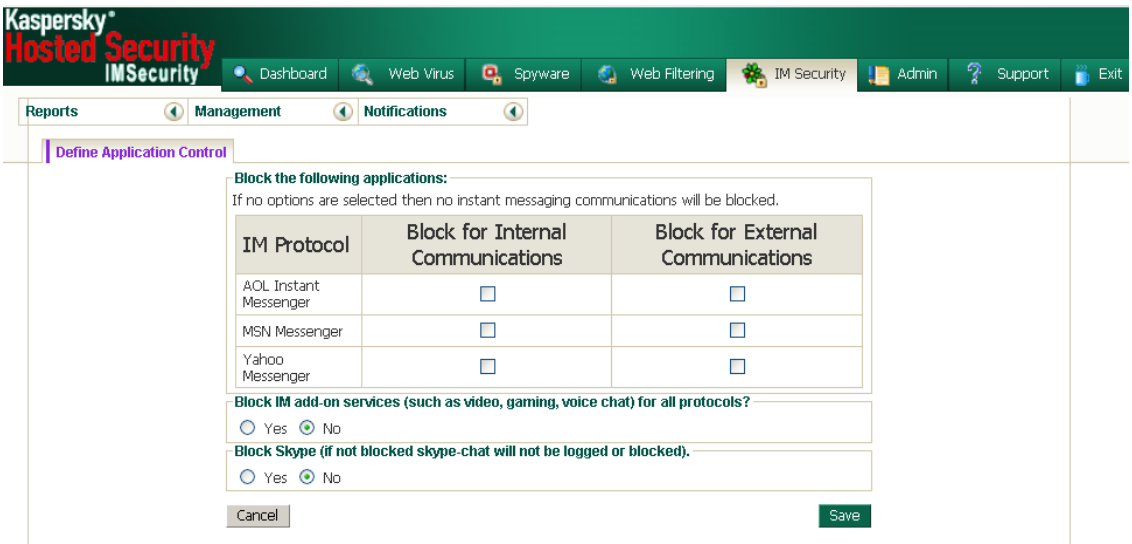
1. Click the 'IM Control' service tab on the main navigation bar at the top of the screen.

2. Click the 'Management' sub-service tab and select the 'Restrictions' button.

3. The main 'Manage Restrictions' page presents you with a listing of all your current restrictions. To review the settings for a particular restriction, click the corresponding restriction in question. The components of the requested Restriction (as detailed at the top of the page) will then appear.

4. Click the 'Define' button in the Applications section.

5. Select check boxes for the corresponding applications (AOL, MSN, or Yahoo Instant Messenger clients) for which you wish to block internal or external communications.



6. Select 'Yes' or 'No' to block add-on IM services (such as video, gaming, voice chat) for all protocols. This will block all additional applications used through the IM Service.

7. Select ‘Yes’ or ‘No’ to block the Skype application for communicating.

8. To save the settings, click the ‘Save’ button. You will then be taken back to the ‘Edit Restrictions’ page. If you hit ‘Cancel’, the operation will be aborted.

For Skype Blocking to successfully work, your network must be configured in the following way.

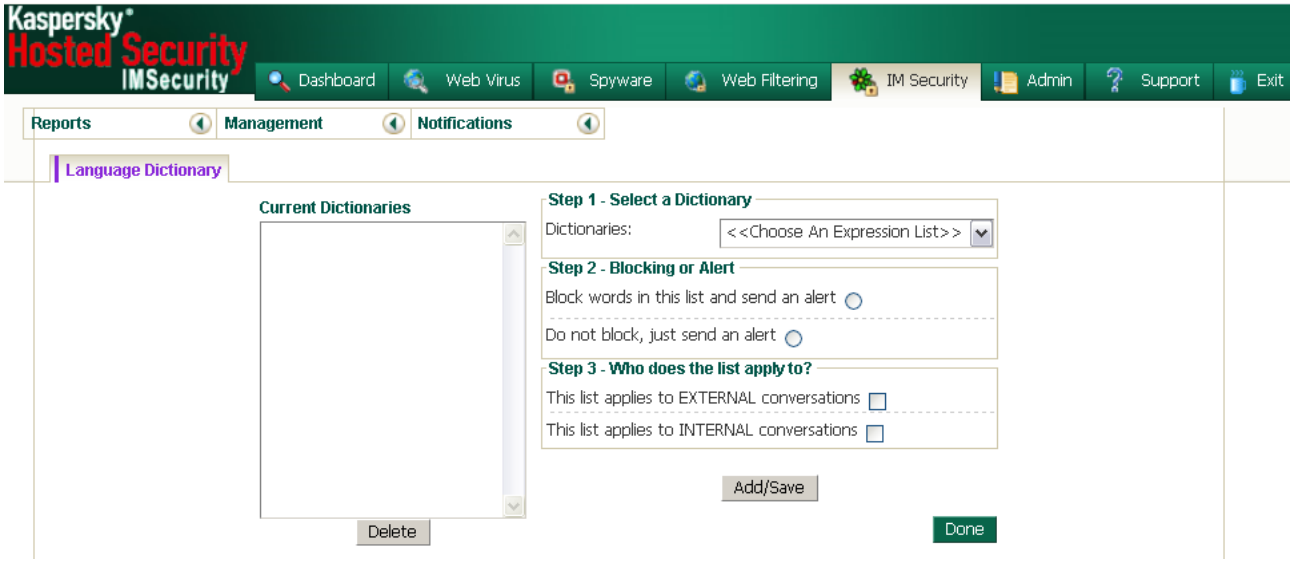
9. You must either being using transparent proxies for HTTP and HTTPS or have firewall rules which only allow HTTP and HTTPS to exit over port 8080 to a Kaspersky Hosted Security tower.

10. Even though you may have the proxy set correctly in Skype, it will always try to connect out to many different servers first, so do not rely on just setting the proxy correctly in the Skype application.

This feature will completely block the login communication of the Skype client, so no features will be available to the end-user including voice and chat communications.

DICTIONARIES. CONFIGURING THE DICTIONARIES YOU WOULD LIKE TO USE FOR BLOCKS/ALERTS

1. Make sure you have selected the required Restriction you wish to edit from the ‘Manage Restrictions’ main page.



2. Click ‘Define’ button in the Dictionaries sub-section in the Edit Restriction page. This will bring up the ‘Language Dictionary’ page.

3. Select the dictionary you wish to be used, then click whether you want to block access and send an alert or not block and just send alerts.

4. Select whether this should only apply to internal conversations or external conversations only.

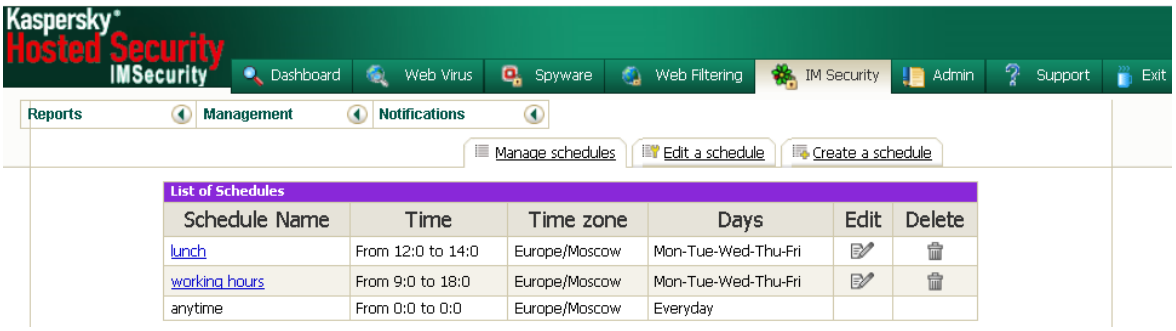
5. Click ‘Add/Save’ to save your changes for the specified dictionary you selected.

6. If you would like to delete a dictionary in use, select a dictionary under the ‘Current Dictionaries for IM’ and click the ‘Delete’ button.

7. When you have finished editing settings for existing dictionaries, click ‘Done’.

SCHEDULES

When implementing IM Control within an organization, you may wish to change the type of Restriction for a group of users based on the time of day and/or day of the week. For example, you might like to let your staff have access to IM only during their lunch hour. Kaspersky Hosted Security facilitates this by enabling you to create a time period (called a Schedule) and then pair that 'Schedule' with a particular Group and 'Restriction' within the 'Dashboard'. In this way, a Group can have many different types of access depending on the time of day and day of the week.



HOW KASPERSKY HOSTED SECURITY PROCESSES SCHEDULES

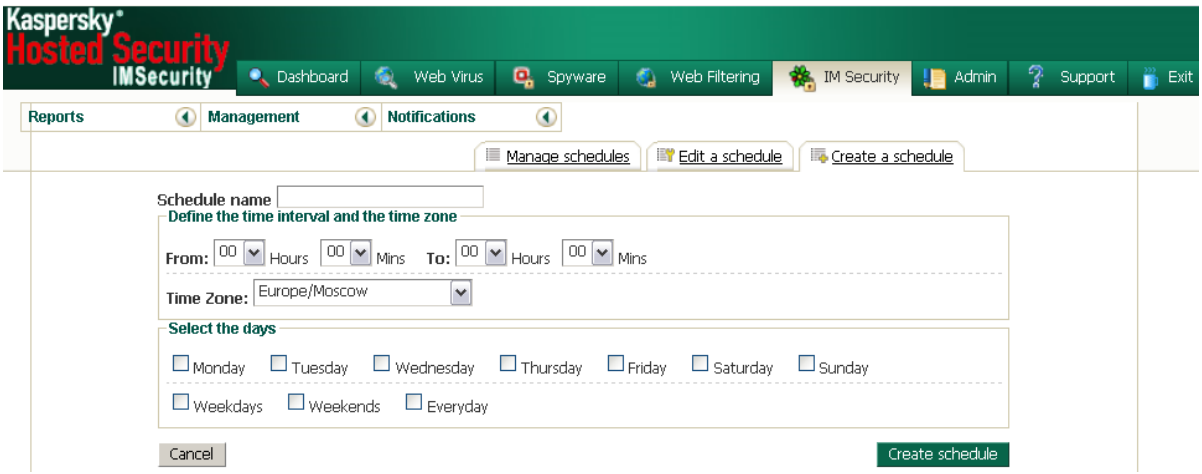
The order of precedence of schedules is based on the length of the defined time period. For example, suppose that you have three schedules:

- Default (24x7)
- Work Day (09:00 – 18:00)
- Lunch (13:00 – 14:00)

The shortest schedule will take precedence over the longest schedule. This means that Kaspersky Hosted Security will look at the Lunch restriction first and if the current time falls between 13:00 – 14:00 then the Restrictions associated with the Lunch Schedule will be applied to the Group. Obviously, if the current time does not fall between 13:00 – 14:00 then the Work Day Schedule will be executed. Finally, if no Schedule encompasses the current time then the Default Schedule will apply. You may wish to set the Schedule associated with the Default time period to block all browsing, by creating a Red List with a '*' entry.

CREATING A SCHEDULE

1. Click the 'IM Control' service tab on the main navigation bar at the top of the screen.



2. Click the 'Schedules' link in the Management sub-service menu. This will bring up the main 'Manage Schedules' page.

3. Click the ‘Add Schedule’ button, which brings up the Add/Edit Schedule.

4. Type the name you wish to give to the new Schedule in the ‘Name:’ text field located at the top of the page.

5. Select the ‘From’ and ‘To’ times that you would like the schedule to encompass, by selecting the hour and or minutes from the respective drop-down boxes provided.

If you would like to create a 24-hour schedule, you must set both the ‘From’ and ‘To’ times to 00hrs 00mins.

6. Use the drop down box to select the time zone for the schedule.

7. Select the days of the week for which you would like the Schedule to be active. This is done by clicking the check boxes located next to each day of the week.

You cannot create a schedule without selecting at least one day of the week.

8. Once you are happy with the settings for your new Schedule, click the ‘Save’ button located at the bottom of the page. Otherwise, click the ‘Cancel’ button to abort and to return to the previous page.

EDITING A SCHEDULE

1. Click the ‘IM Control’ service tab on the main navigation bar at the top of the screen.

2. Click the ‘Schedules’ link in the Management sub-service menu. This will bring up the main ‘Manage Schedules’ page.

3. The main ‘Manage Schedules’ page presents you with a listing of all your current schedules. To edit an existing schedule, click the existing schedule in question.

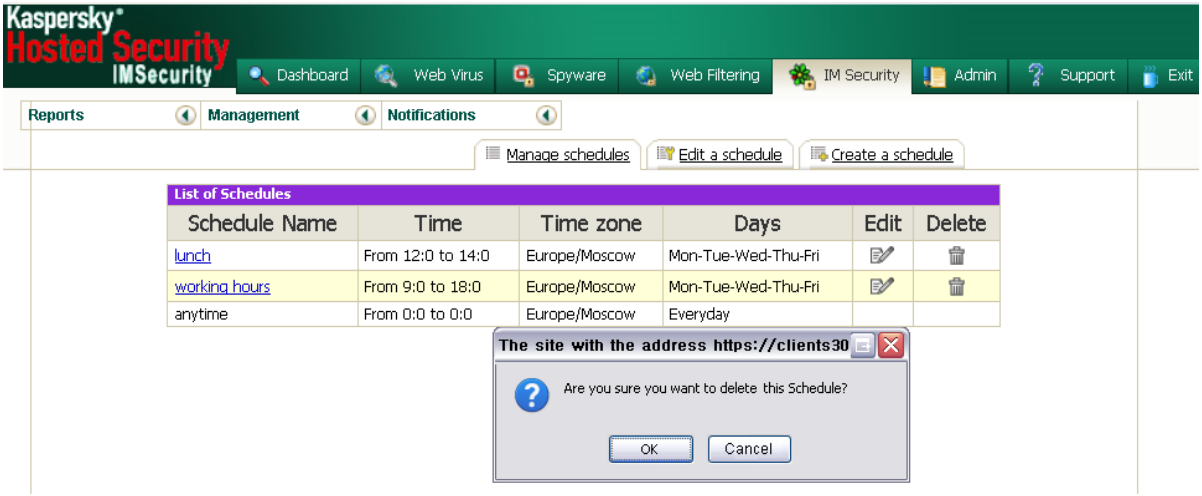
4. Modify the settings of the Schedule and click ‘Save’ to save the configuration. You will be returned to the previous page. Otherwise, click the ‘Cancel’ button to abort and to return to the previous page.

DELETING A SCHEDULE

1. Click the 'IM Control' service tab on the main navigation bar at the top of the screen.

2. Click the 'Schedules' link in the Management sub-service menu. This will bring up the main 'Manage Schedules' page.

3. The main 'Manage Schedules' page presents you with a listing of all your current schedules. To delete an existing schedule, click the corresponding check box under the Delete column. Then, click the 'Delete Schedules' button. A validation message will appear to ask if you are sure you want to delete the selected reports; click 'OK' to delete the reports.

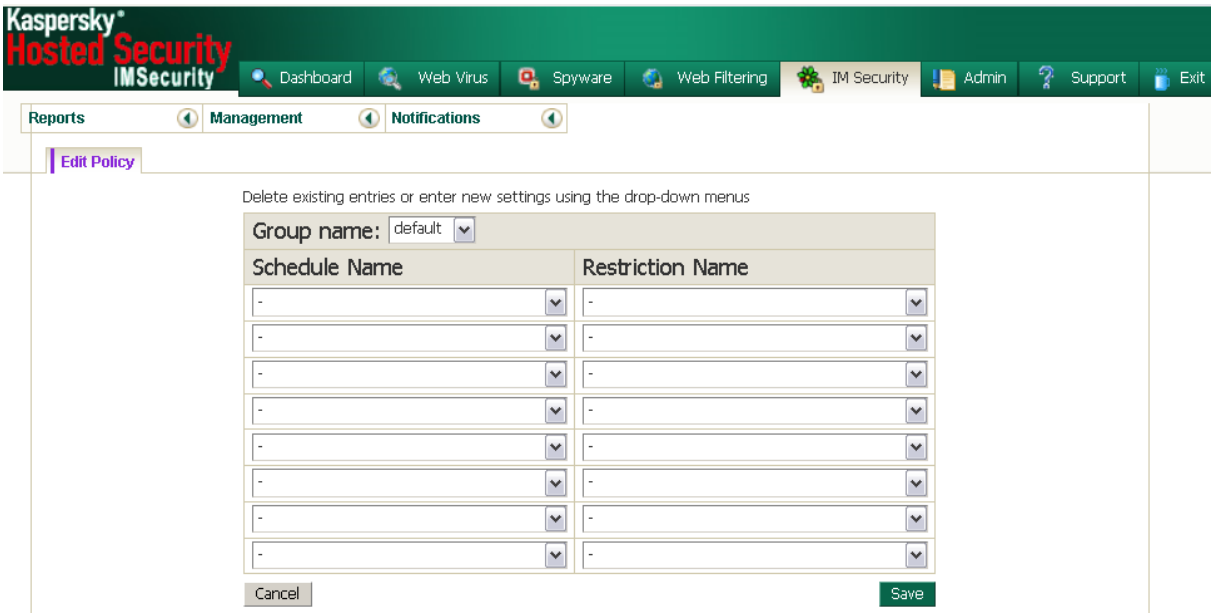


4. The deleted access restriction will no longer be displayed in the list on the main 'Schedules' page.

If the schedule you have chosen to delete has one or more pairings associated with it in the dashboard, Kaspersky Hosted Security will not let you delete it.

POLICIES

The 'Manage Policies' page provides you with a visual overview of the IM Control settings you have configured for your organization. The simple layout enables you to see all the User Groups, Restrictions, and Schedules. Each combination of a Restriction and a Schedule within the Policies page is referred to as a Pairing. Each Policy must consist of at least one pairing along with a single Group name. To create a typical, time-dependent policy, multiple pairings can be used.



CREATING A POLICY

You cannot create a new pairing unless you have first created at least one 'Schedule'.

1. Click the 'IM Control' service on the main navigation bar at the top of the screen.
2. Click the 'Policies' link in the Management sub-service tab.
3. Click the 'Add Policy' button located at the bottom of the page. You will then be taken to the 'Edit Policy' page.
4. This page consists of three sets of pull-down menus side by side: one for selecting a 'Group Name', and up to five each for Schedules and Restrictions. If you are creating a new pairing, simply select required Group Name and add the Schedule and Restriction Names as required.
5. Click 'Save' to save the pairings to return to the Policies window. Otherwise, click 'Cancel' to abort and to return to the Manage Policies window.

EDITING A POLICY

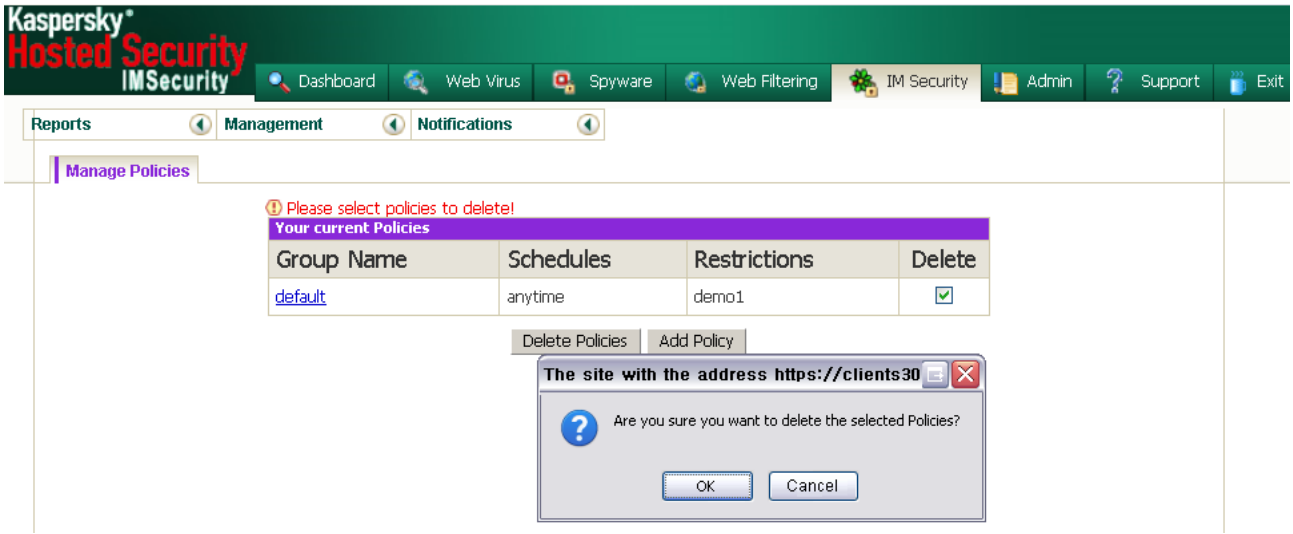
1. Click the 'IM Control' service on the main navigation bar at the top of the screen.
2. Click the 'Policies' link in the Management sub-service tab.
3. Click the corresponding existing policy link to edit the policy. You will then be taken to the 'Edit Policy' page.
4. Click Delete to remove existing pairings and select required Group Name and add the Schedule Name and Restriction Names as required.

5. Click ‘Save’ to save the pairings to return to the Policies window. Otherwise, click ‘Cancel’ to abort and to return to the Manage Policies window.

DELETING A POLICY

1. Click the ‘IM Control’ service on the main navigation bar at the top of the screen.

2. Click the ‘Policies’ link in the Management sub-service tab.



3. Find the pairing within the listed Policies that you want to delete, and then click the checkbox in the Delete column located to the right of the policy.

4. You will then be presented with a pop-up dialog box asking you if you are sure you want to delete the pairing. Click the ‘OK’ button to proceed.

5. You should now se e that the pairing is no longer listed in the ‘Manage Policies’ listing.

If you want to delete the entire Policy, simply delete each pairing within the policy.

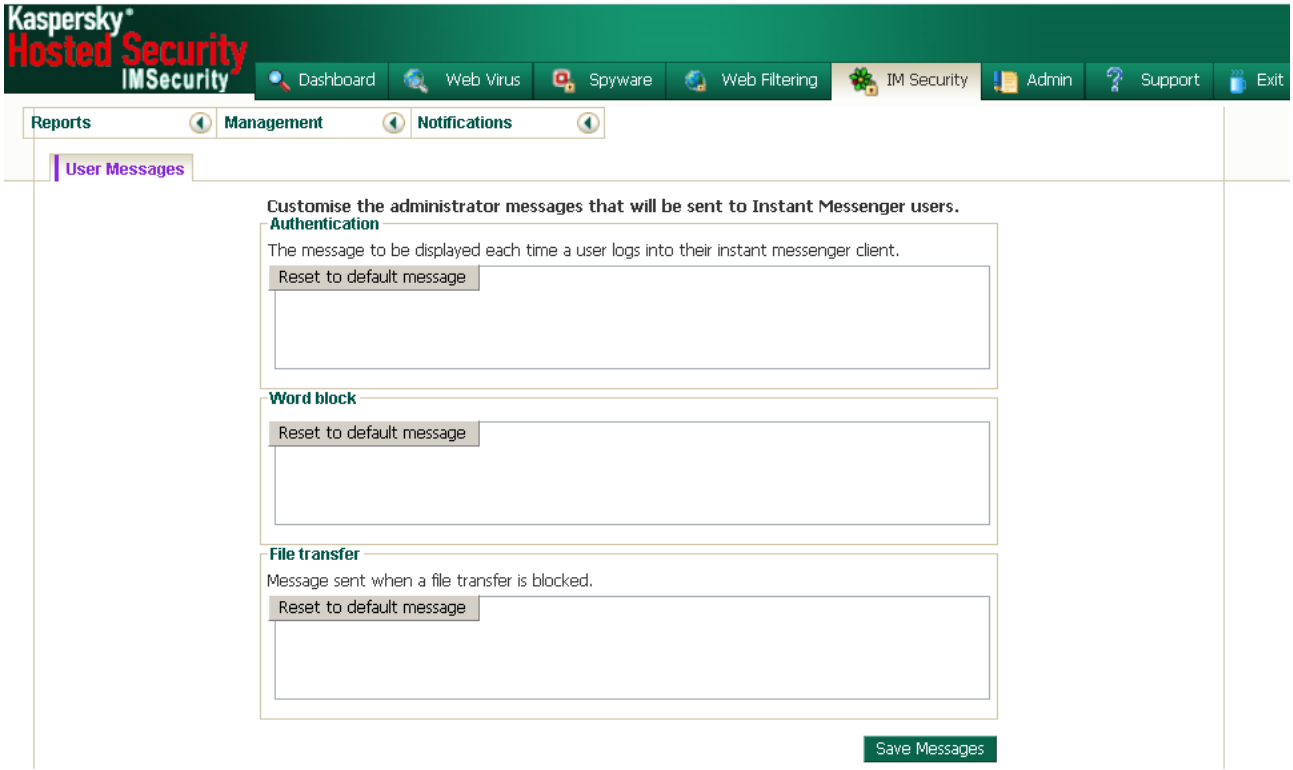
IM CONTROL NOTIFICATIONS

Under the Notifications sub-service tab, there are currently two options which will require configuration:

- **User Messages**: this lets you specify the message which an end-user will see when a request is blocked.
- **Email Alerts**: this enables an administrator to receive an email alert for blocked activity.

IM CONTROL USER MESSAGES

The Kaspersky Hosted Security User Message is the page that your users will see when they log into their IM client, when a virus is detected, when a word has been blocked, and when a file transfer has been blocked while they are using their IM client. You can append your own information to the Alert Page in order to customize it for your organization. For example, you may wish to add the System Administrator's contact details, or links to your organization's IM filtering and security policy.



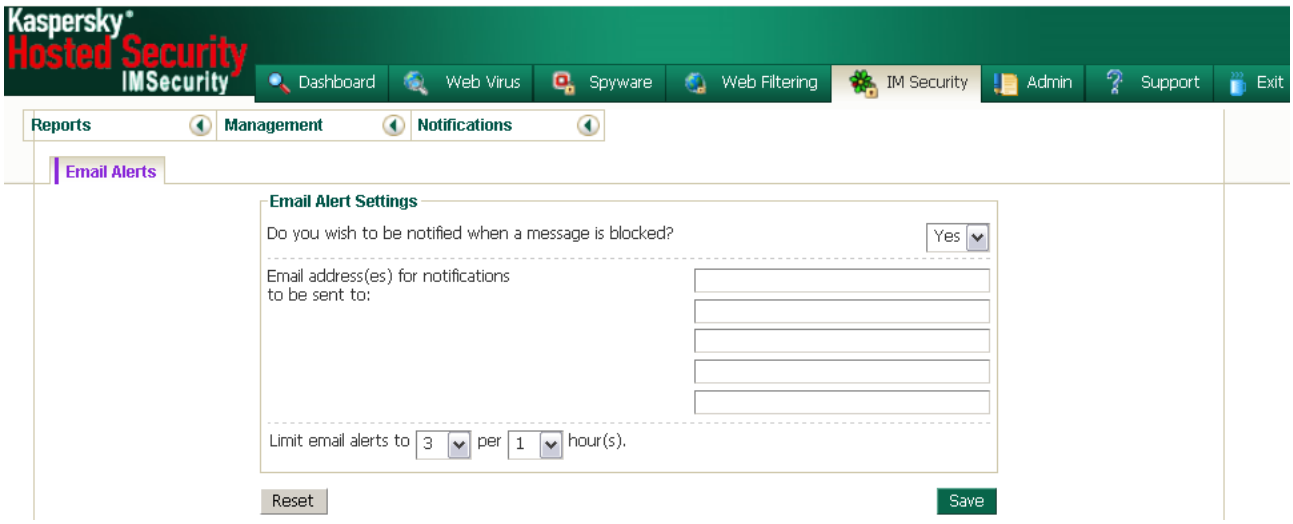
The custom information must be submitted in HTML.

1. Click the 'IM Control' tab on the main navigation bar at the top of the screen.
2. Click the 'User Messages' link in the Notifications sub-service tab.
3. Type or cut and paste the additional messages into the empty text area for each section: Authentication, Virus Transfer, Word Block, and File Transfer.
4. Once you are happy with the User Messages modifications you have made, click the 'Save Messages' button located at the bottom of the screen.

IM CONTROL EMAIL ALERTS

The IM Control E-mail Alerts are emails that notify you of when Kaspersky Hosted Security has blocked a page. The email will contain the following information:

- The IP address from which the request left your organization.
- The Internal IP address and or the user/group (if available – requires installation of a Connector).
- The reason the requested message was blocked.
- The IM address to which the IM was sent.



EMAIL GENERATION

1. Click the 'IM Control' service tab on the main navigation bar at the top of the screen.

2. Click the 'Email Alerts' link in the Notifications sub-service. This will bring up the 'E-mail Alerts' page.

3. Select whether or not you want to be notified when a page is blocked by selecting 'Yes' or 'No' from the drop down box.

4. Enter the email address (or addresses) you want notifications to be sent to in the empty text fields provided. You can specify a maximum of five different email addresses that you wish to have these alerts sent to. If you require the alerts to be sent to any more addresses than this, we recommend that you set up a group mailing address.

5. If you wish to throttle the amount of email alerts you receive, click in the box next to the statement 'Limit these alerts to'. Throttling will now be activated and you must then select the number of alerts you wish to receive, per the amount of hours you specify. For example, you might decide that you only ever want to get a maximum of three email alerts in any two-hour period.

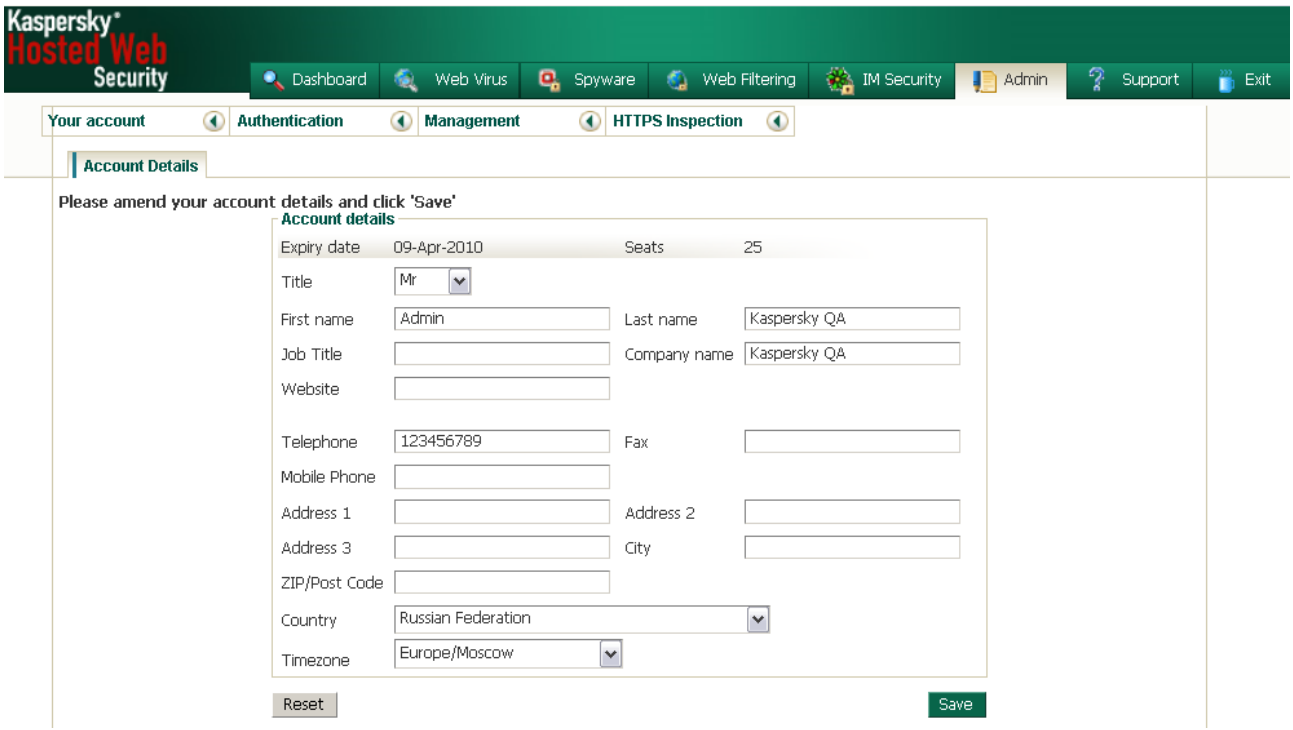
6. Once you are happy with the E-mail Alert details you have entered, click the 'Save' button located at the bottom of the screen.

ADMINISTRATION

EDITING YOUR ACCOUNT DETAILS

- Click the 'Admin' tab on the main navigation bar at the top of the screen. You will be presented with the 'Account Details' page.

- The form on the 'Account Details' page is self-explanatory; fill in the required contact details and then click the 'Save' button located at the bottom of the page.



GROUP MANAGEMENT

The 'Groups' link in the Management sub-service tab is used to create and define Custom Groups and Directory Groups. Groups are used to segment an organization's user base so that more granular, or role specific, web usage policies can be enforced. Kaspersky Hosted Security uses two types of Groups to achieve this functionality:

- **Directory Groups**: as the name implies, a Directory Group represents a group of users as defined by a WinNT domain or by Active Directory. Typically a Directory Group will represent a group of users with similar roles (hence access privileges) within the organization.

- **Custom Groups**: these are defined by either (or both) usernames and IP addresses and subnets. Usernames are specified according to the WinNT or Active Directory schema. IP addresses can be private (publicly non-routable) or public.

Each of these groups will be discussed in further detail. It should be noted that in order for either of these group based web access controls to function, you must have a Connector installed within your infrastructure. If the Connector is not installed, all Web requests will be managed by the default policy and an Alert page that is displayed to users within your organization when Web content is blocked.

HOW KASPERSKY HOSTED SECURITY EVALUATES/PRIORITIZES GROUPS

Kaspersky Hosted Security evaluates groups using a fast, multi-stage selection process, which accommodates variations in customer infrastructure and the Connector configuration.

1. If the Connector has been configured to send internal group details, then a check will first be made to see if the supplied group name matches any groups configured within Kaspersky Hosted Security. If such a match exists, the matched group will be selected. If the user belongs to more than one group, then any group containing the string 'webscan' will take precedence.

2. If the group name is absent or unmatched, but user name details are present, then a further check is made to see if the username has been configured within an existing group.

3. If the group is still unmatched, and the internal IP address is present, then a further attempt is made to match the internal IP address with a group IP Expression.

4. If the group is still unmatched, then a further attempt is made to match the external IP address with a group IP Expression.

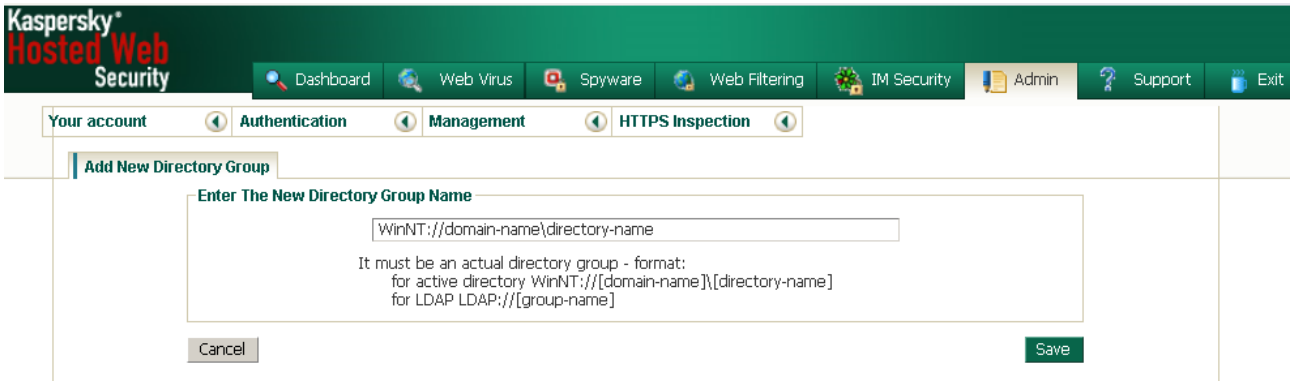
5. Finally, if no match has been made, then the 'default' group is selected.

CREATING A DIRECTORY GROUP

1. Click the 'Admin' service tab on the main navigation bar at the top of the screen.

2. Click the 'Groups' button in the 'management' sub-service tab. This will bring up the 'Groups' screen.

3. Click the 'Add Directory Group' button at the bottom of the screen. You will then be presented with a screen in which you can enter in a new 'Directory Group Name'.



4. Type the name of the group into the provided text field. You must use the following syntax when specifying a WinNT or Active Directory group:

   WinNT://DOMAIN_NAME\GROUP_NAME

   WinNT://ACTIVE_DIRECTORY_REALM\GROUP_NAME

5. The syntax is case insensitive and there may be spaces in the names. However, the names should be spelled exactly as they appear within your Windows Domain or Active Directory.

6. To create the new Directory group, click the 'Save' button. You will then be taken back to the main 'Manage Groups' page where you will see your new Directory Group in the Groups list.

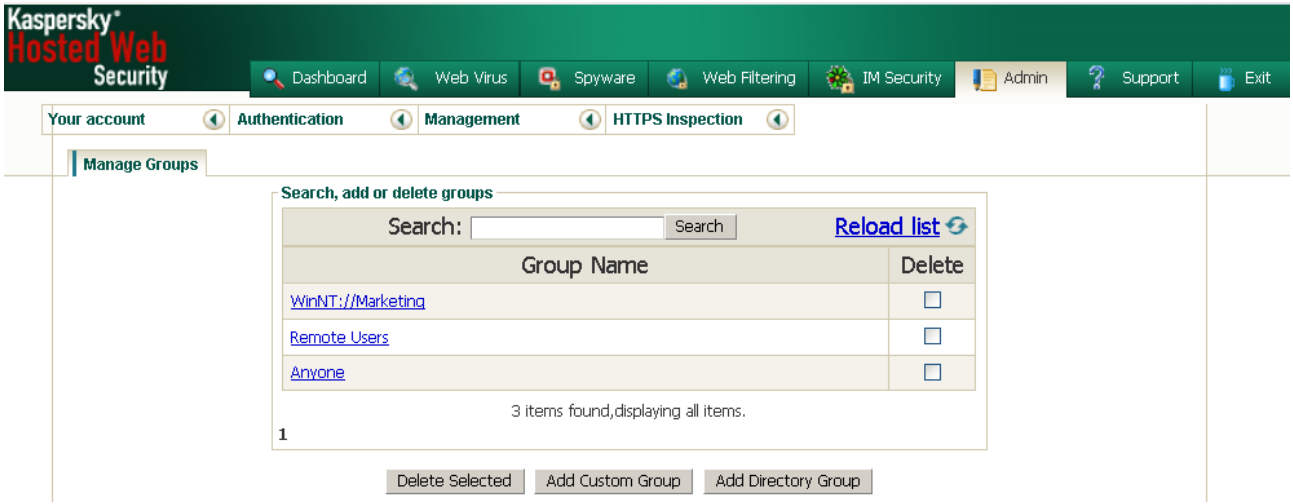
The Directory Group name, itself, is functional and therefore no further parameters are required to configure the Directory Group.

EDITING A DIRECTORY GROUP NAME

1. Click the 'Admin' service tab on the main navigation bar at the top of the screen.

2. Click the 'Group' button in the 'management' sub-service tab. This will bring up the 'Groups' screen.

3. Click the group button which corresponds to the Directory Group which name you want to change.



4. Edit the name of the Directory Group in the text field. You must use the following syntax when specifying a Windows NT or Active Directory group:

   WinNT://DOMAIN_NAME\GROUP_NAME

   WinNT://ACTIVE_DIRECTORY_REALM\GROUP_NAME

5. The syntax is case insensitive and there may be spaces in the names. However, the names should be spelled exactly as they appear within your Windows Domain or Active Directory.

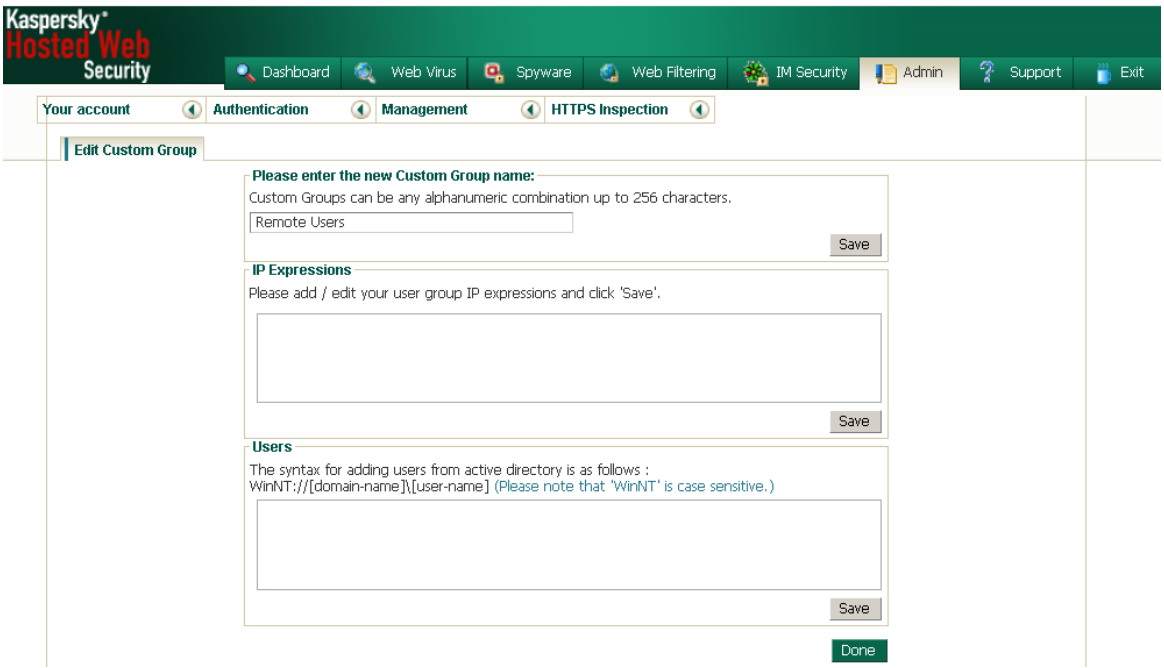
6. To save the new Directory group, click the 'Save' button. You will then be taken back to the main 'Manage Groups' page where you will see your new Directory Group in the Groups list. Clicking the 'Cancel' button will abort any changes and return you to the previous Groups page.

CREATING A CUSTOM GROUP

1. Click the 'Group' button in the 'Management' sub-service tab. This will bring up the 'Groups' screen.

2. Click 'Add Custom Group'.

3. Enter the name of the Custom Group you wish to create into the 'Custom Group' text field.



4. To register the new Custom Group, click the 'Save' button. You will then be taken back to the main 'Manage Groups' page where you will see the new Custom Group name in the groups list. If you hit 'Cancel', the operation will be aborted and you will return to the groups list.

5. You should now add either (or both) IP Addresses or User Names to the Custom Group. Each of these procedures is detailed below.

ADDING OR EDITING USERNAMES FOR A CUSTOM GROUP

1. Click the corresponding button for the group you have already created on the Group listing page.

2. Enter the user names of all the users you would like in the group, putting each on a separate line within the text area provided. You must use the following syntax when specifying a Windows NT or Active Directory user:

   WinNT://DOMAIN_NAME\USER_NAME

   WinNT://ACTIVE_DIRECTORY_REALM\USER_NAME

   The syntax is case insensitive and there may be spaces in the names. However, the names should be spelled exactly as they appear within your Windows Domain or Active Directory.

3. To save the entered usernames, click the 'Save' button. Otherwise click 'Cancel' to abort the entries and to return to the Manage Groups page.

CREATING A GROUP USING IP ADDRESSES

1. Click the corresponding existing group button on the Group listing page.

2. Enter the IP expressions, into the text area, that are required to identify the users you want in the group. The expressions you can use are as follows:

   Individual IP addresses, each on a new line (e.g. 192.168.0.25)

   Network Masks, each on a new line (e.g. 192.168.0.0/255.255.255.0)

3. To save the entered IP Addresses (and subnets), click the 'Save' button. Otherwise click 'Cancel' to abort the entries and to return to the Manage Groups page.

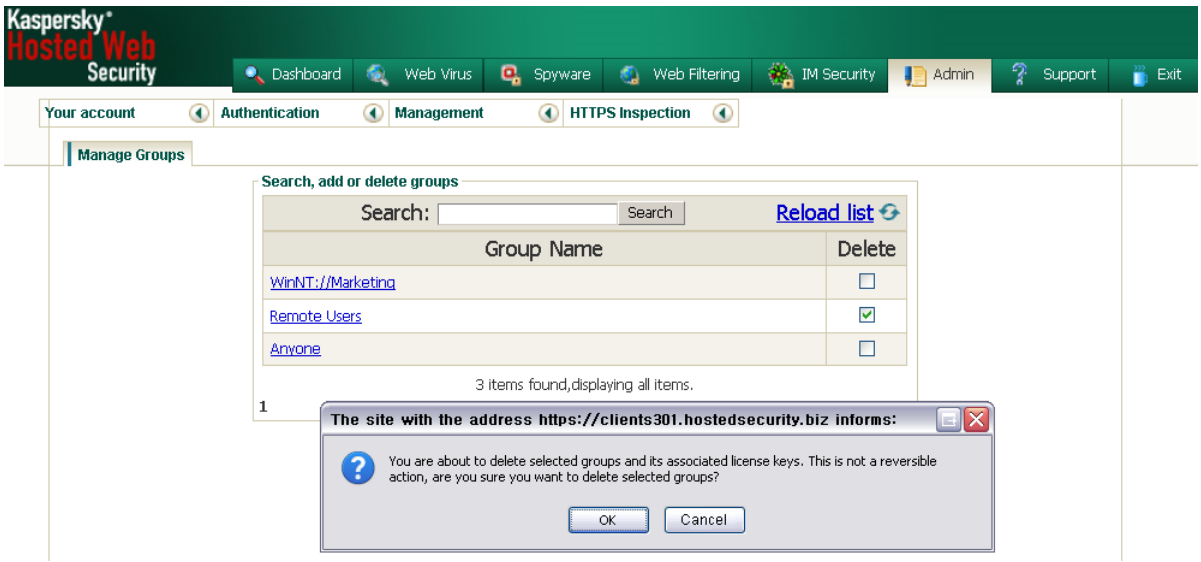
DELETING A GROUP

1. Click the 'Admin' service tab on the main navigation bar at the top of the screen.

2. Click the 'Groups' button in the 'Management' sub-service tab. This will bring up the 'Manage Groups' page listing all the existing groups.

3. Click the checkbox next to the selected existing group you wish to remove in the Delete Column. Then click the 'Delete Groups' button.

4. A dialog box will appear, asking if you are sure you want to delete the user group. Click the 'OK' button to proceed with deletion. The deleted group will no longer be displayed on the main Manage Groups page.



The user group you have chosen to delete has one or more pairings associated with it in the Policies listing, then Kaspersky Hosted Security will not let you delete it.

THE DEFAULT GROUP

If a user has not been assigned to a specific group, the user will automatically become a member of the Default group. The Default group cannot be deleted and you cannot add 'Users' or 'IP Expressions'.

DUPLICATE USERS OR IP ADDRESSES

The administrator should avoid duplicating Domain/Active Directory usernames or IP addresses across different Custom Groups. If you do duplicate any of these parameters, then the first group found will determine web access policy for that user.

AUTHENTICATION KEY MANAGEMENT

Kaspersky Hosted Security Authentication Keys are used in conjunction with an installation of a Connector. Connectors identify end users by merging user details from Active Directory using LDAP or Windows Domain integration and the applied Authentication Key for the Connector. Connectors enable users to connect to the Kaspersky Hosted Security Web Services with either a static IP address (no authentication key required) or a dynamic IP address by using a Company, Group, or User Authentication Key.

Connectors can encrypt user information and the Kaspersky Hosted Security Web Services can apply specific user or group policy information based on this information. Connectors pass end-user Web traffic requests through the Kaspersky Hosted Security Web Services for filtering, scanning, and policy enforcement, before providing the cleansed Web content back to the end-user. You can find more information about Connectors in the Connector Installation Guide.

Authentication Keys can be created via Kaspersky Hosted Security under the Admin tab. You can create a Company, Group, or User Authentication Key which will be used to identify and authenticate the user to the Kaspersky Hosted Security Web Services. A User Authentication Key enables more detailed user behavior reporting and policy management, but requires administrators to manage more keys.

Authentication Keys are also used with the Anywhere+ roaming solution.

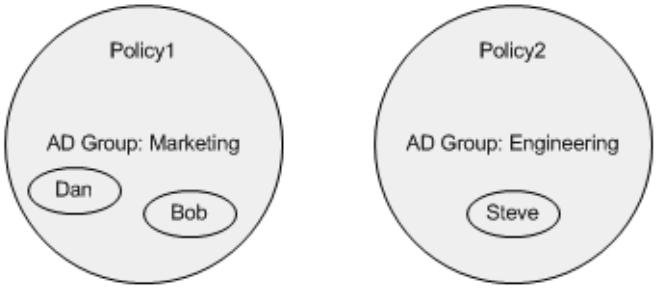
CONNECTOR AND AUTHENTICATION KEY DEPLOYMENT SCENARIOS

Here are three examples of the most popular deployment scenarios for Connectors using Company, Group, and User Authentication Keys.

CASE 1: COMPANY AUTHENTICATION KEY AND ACTIVE DIRECTORY (MOST POPULAR SCENARIO)

Scenario Setup

- Two AD groups created in Kaspersky Hosted Security:
  - WinNT://…/Marketing
  - WinNT://…/Engineering
- Company Authentication Key and Connector installed on Domain Controller.
- Policy1 applied to Marketing and Policy2 applied to Engineering.



Scenario Questions & Answers

- What policy will apply to Dan, Bob, and Steve?
    - Policy1 is applied to Dan and Bob, and Policy2 is applied to Steve.
- If a policy causes a block, what group will be registered against the block?
    - Blocks for Dan and Bob are registered against group WinNT://…/Marketing with user information for Dan and Bob.
    - Blocks for Steve are registered against group WinNT://…//Engineering with user information for Steve.

CASE 2: GROUP AUTHENTICATION KEY

Scenario Setup

- There are three branch offices and they do NOT currently use Active Directory groups. A connector is installed at each branch office, with a group authentication key installed for each workgroup connector coordinating to each office.
- Group Authentication Keys: SFGROUP, LONDONGROUP, SYDNEYGROUP
- Policy1 applied to SFGROUP, Policy2 applied to LONDONGROUP, Policy3 applied to SYDNEYGROUP.

Scenario Questions & Answers

- What policy will apply to Dan, Bob, Jim, and Joe?
    - Policy1 is applied to Dan and Bob.
    - Policy2 is applied to Jim.
    - Policy3 is applied to Joe.
- If a policy causes a block, what group will be registered against the block?
    - Blocks will be registered against the group SFGROUP for Dan and Bob.

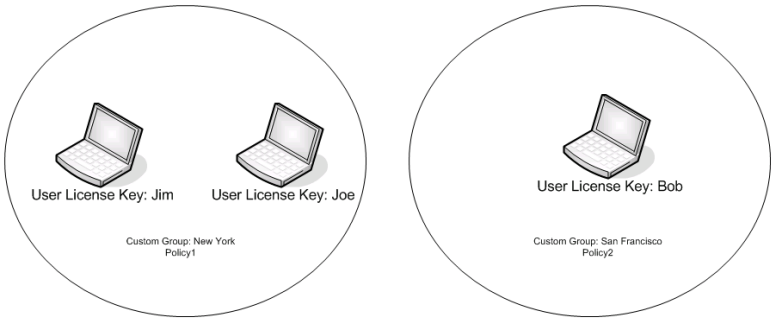
- Blocks will be registered against the group LONDONGROUP for Jim.
- Blocks will be registered against the group SYDNEYGROUP for Joe.

If you are using Active Directory, you are advised to use Case 1 (Company Authentication Key) to appropriately apply group policy.

CASE 3: USER AUTHENTICATION KEY

Scenario Setup

- There are three mobile laptop users for whom you want to apply Kaspersky Hosted Security Web Services protection to while the user is surfing the Web remotely at home or traveling (outside the corporate network). The Connector is installed on each of these laptops, and the User Authentication Key for each laptop identifying each user.
- Custom Groups: New York and San Francisco
- User License Keys: Jim, Joe, Bob



Scenario Questions & Answers

- What policy will apply to Jim, Joe, and Bob?
  - Policy1 will be applied to Jim and Joe in the New York Custom Group.
  - Policy2 will be applied to Bob in the San Francisco Custom Group.
- If a policy causes a block, what group will be registered against the block?
  - Blocks registered against New York custom group and as user Jim and Joe.
  - Blocks registered against San Francisco custom group and as user Bob.

User Authentication Key overrides all user information reported, so only use ONE user license key per ONE connector on ONE system.

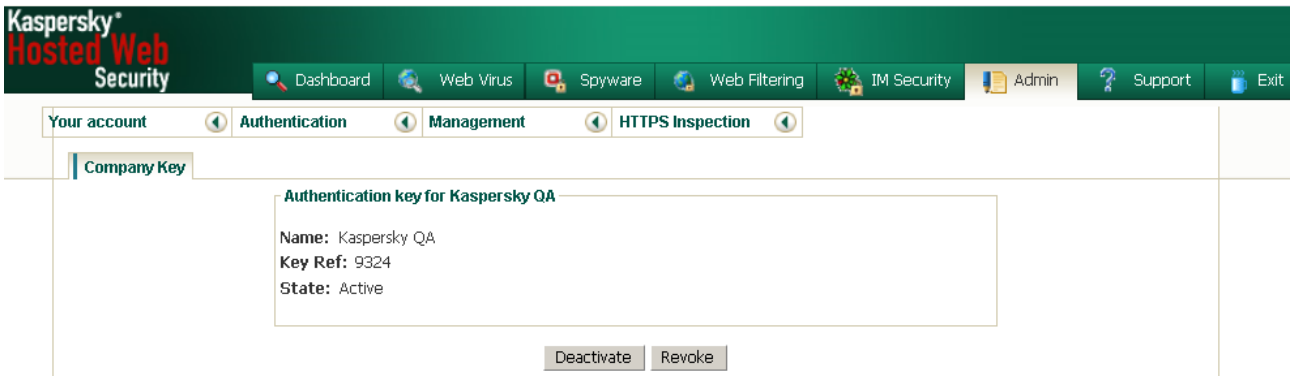
SUMMARY

- If you want to use Active Directory for granular policy and user reporting, you should use the Company key installed on the Domain Controller with an Enterprise or Workgroup Connector.
- If you have satellite offices where you want to apply a group policy to everyone in that office, you should use the Group Authentication Key.
- If you have mobile laptops or systems, you should use the User Authentication Key on a 1:1 basis.

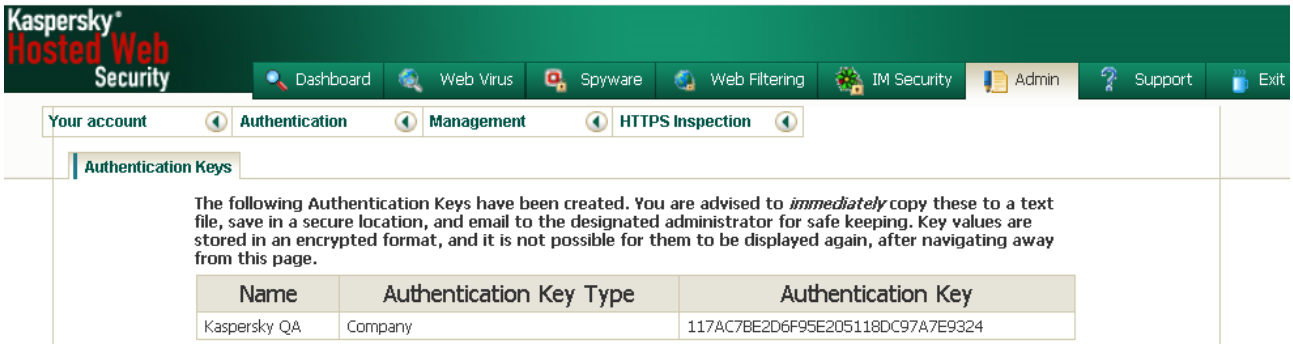
With the launch of Anywhere+, Kaspersky Hosted Security no longer recommends the use of the Connector on mobile laptops. Please contact your Kaspersky Hosted Security representative for more information on the Anywhere+ roaming.

CREATING AND DELETING AUTHENTICATION KEYS

In most cases, the Company Authentication Key is the only key you need to create. If you want to use Active Directory for granular policy and user reporting, you should use the Company key installed on the Domain Controller with an Enterprise or Workgroup Connector. There can be only one Company Authentication Key.



If you wish to create individual Group or User Authentication Keys, you must create your group and user structure using the Groups Sub-Service Link first before you create the group or user authentication keys. Your definition of your group and users are used to populate the available types of authentication keys you may create.


Kaspersky Hosted Web Security
Dashboard
Web Virus
Spyware
Web Filtering
IM Security
Admin
Support
Exit
Your account
Authentication
Management
HTTPS Inspection
Authentication Keys
The following Authentication Keys have been created. You are advised to immediately copy these to a text file, save in a secure location, and email to the designated administrator for safe keeping. Key values are stored in an encrypted format, and it is not possible for them to be displayed again, after navigating away from this page.
Name
Authentication Key Type
Authentication Key
Kaspersky QA
Company
117AC7BE2D6F95E205118DC97A7E9324

When you begin to create Authentication Keys, the screen will show all available Authentication Keys you may create. If, for example, the Company Authentication Key is not available in this screen, this means that the Company Authentication Key has already been generated.

CREATING AN AUTHENTICATION KEY

1. Click the 'Admin' tab and click the type of Authentication Key you would like to create under Authentication (Company, Group or User).

2. Click 'Create Key' by the Company/Group/User for which you want to have one created.

3. Copy and paste the entire Authentication Key text into a text file application such as notepad.exe and save the file for safekeeping. You will need to copy and paste this key into the Connector configuration when you are installing the Connector.

4. Email the authentication key information to a selected email address.

If you click send, you will not be able to return to this screen – so ensure you saved the Authentication Key information before you click send. If you fail to do this you will need to revoke the key you just created and go through these steps.

DEACTIVATING AN AUTHENTICATION KEY

1. Click the 'Admin' tab and click the type of Authentication Key you wish to deactivate under 'Authentication'.

2. Look for the Authentication Key you wish to deactivate and click the corresponding 'Deactivate' button, which will not delete the Authentication Key, but sets the Authentication Key state to 'Inactive'.

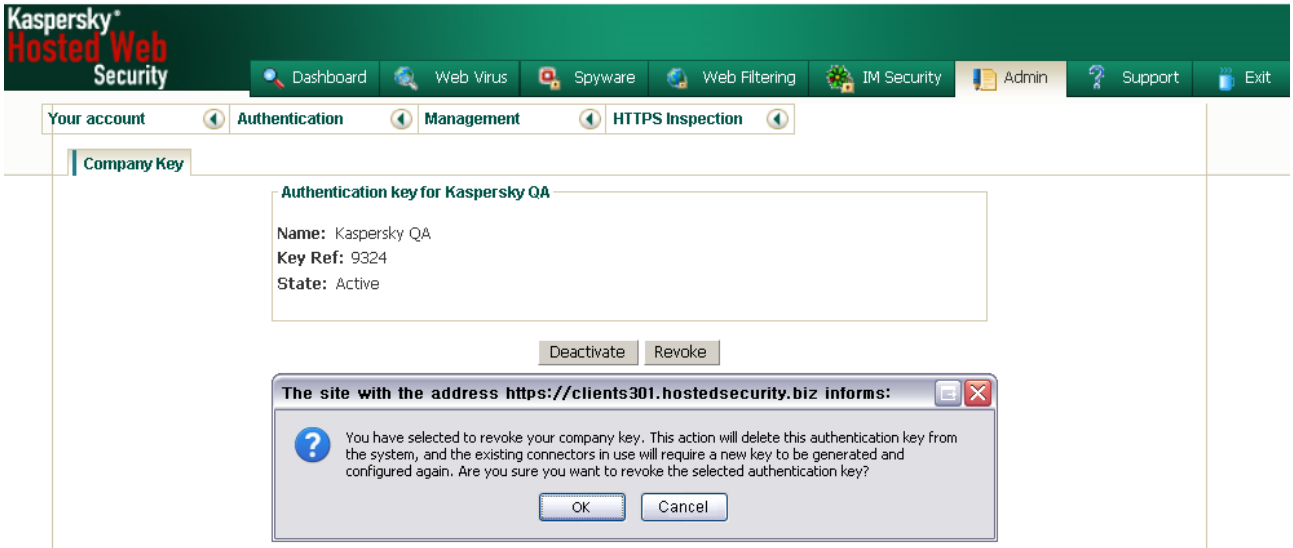
If you are having Forbidden 403 HTML errors in your Web browser while trying to connect to the Internet through the Connector, you should check your Authentication Key activation status; it should state 'Active' to operate properly.

REVOKING AN AUTHENTICATION KEY

Some users may want to remove an Authentication Key for security purposes or for administration needs. Revoking an existing Authentication Key will delete it permanently, and existing Connectors will require re-configuration with a new and Active Authentication Key to operate properly.

1. Click the 'Admin' tab and click the type of authentication key you wish to revoke.

2. Select the Authentication Keys you wish to delete.



3. Clicking the 'Revoke' button at the bottom of the screen.

4. A validation message will appear to ensure you wish to delete the key. Revoking the key is an irreversible action; ensure you are prepared to delete the key before clicking 'OK'. A less severe way of managing Authentication Keys would be to deactivate the key for a period of time, and then revoke the Authentication Keys at a later point.

5. If you wish to revoke the selected Authentication Keys, click 'OK'.

MOBILE SETTING FOR USER AUTHENTICATION KEYS

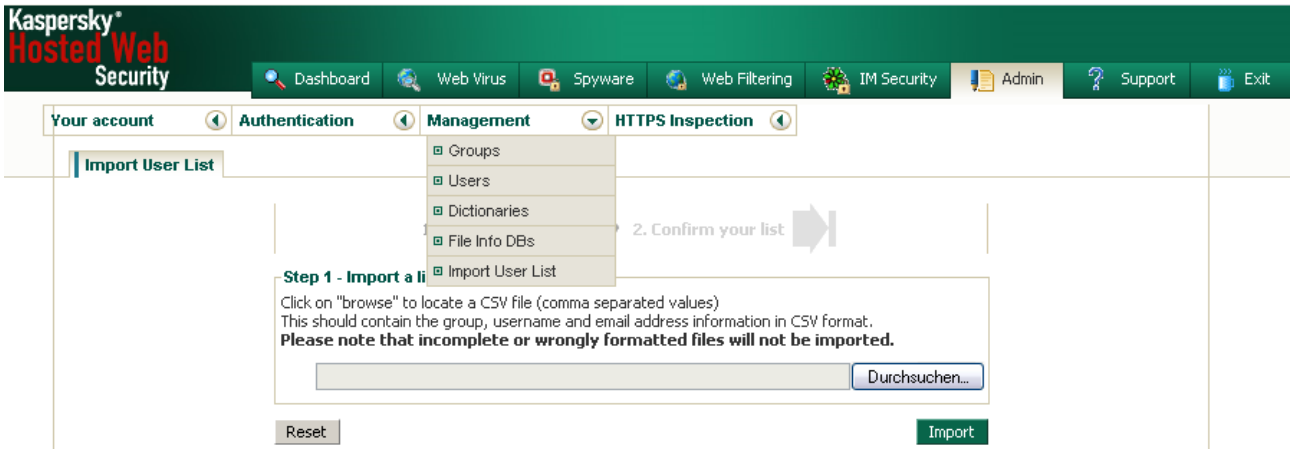
On the user key screen you will see that there is a check box by each user to state if they are an Anywhere+ user. This should only be checked if you are using the Anywhere+ in user mode with this key, not any other type of connector including the Virtual Connector.

IMPORTING A USER LIST

Kaspersky Hosted Security allows administrators to import a list of users and have multiple authentication keys generated in one action. This is achieved by the following.

1. Click the 'Admin' tab.

2. Under the 'Management' menu, click 'Import User List'. The screen shown opposite will appear.

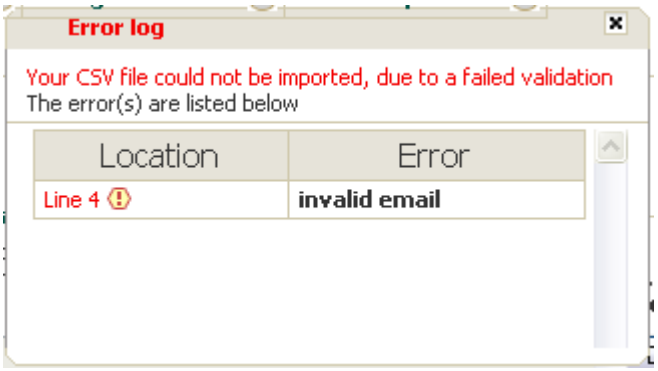


3. Click the 'Browse' button and choose the CSV file you wish to import.

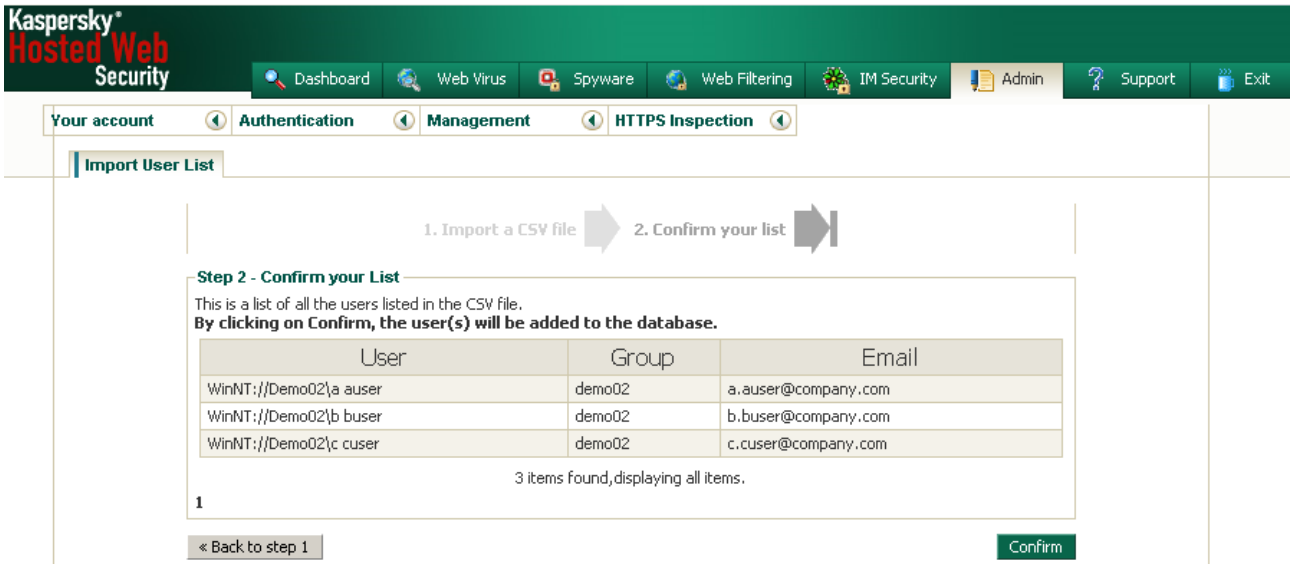
   CSV file is in the format of group, username (must be full directory format e.g. WinNT://engineering\spencer parker), email address

   The CSV file can be no larger than 100 rows.

4. Click the 'Import' button to continue to step 2. If there is a problem with the CSV file it will return an error. Clicking the error log will display the reasons why the file failed.



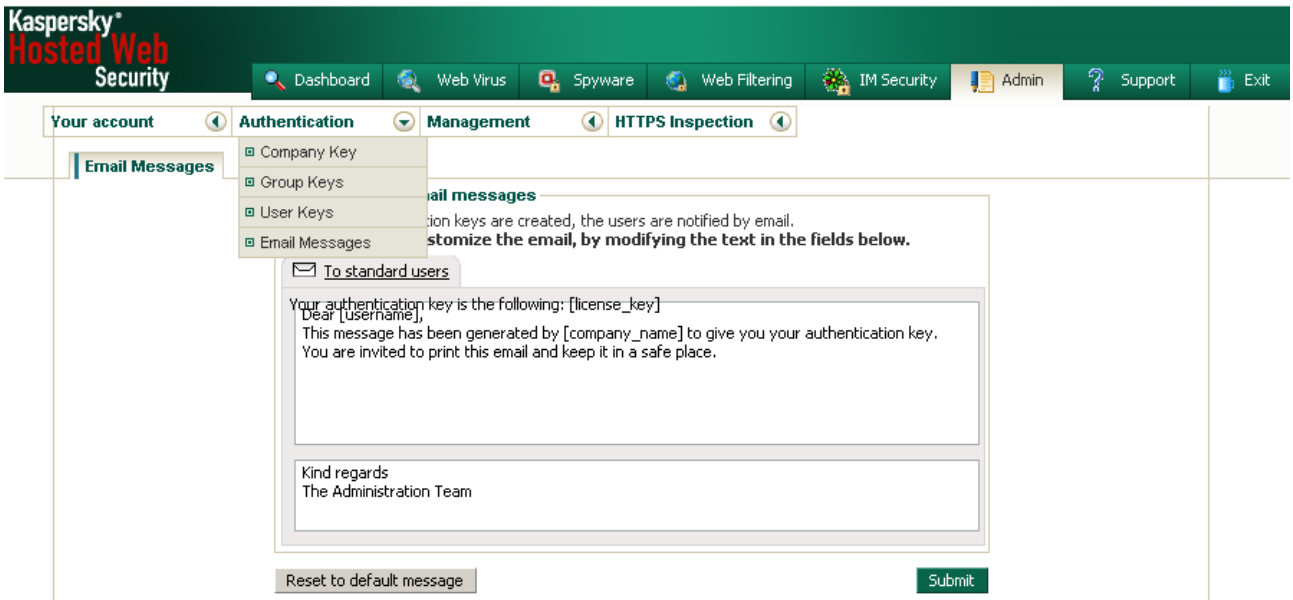
The following screen will appear if the CSV file is correct.



5. Click the 'Confirm' button to add these users. An email will be sent to each user using the email template created (see below). If a user already has a key, then this current key will be revoked and a new one created. If the user appears in a different group, the user will be moved to the new group.

EMAIL MESSAGES

Kaspersky Hosted Security allows administrators to change the standard email template text which is sent to users on the creation of new authentication keys. To do this, please go to the 'Admin' section, click the 'Authentication' menu and click 'Email Messages'. The following screen will appear.



The email has a header and footer which wraps around the authentication key. These can be changed. You can also insert the username by using [username] and the company name by using [company_name]. Kaspersky Hosted Security recommends that you send a test email to check it is formatted correctly before sending it to end-users.

APPENDIX: FILTERING CATEGORIES

Alcohol

Includes Web sites that deal with alcohol as a pleasurable activity (e.g. wine, beer, liquor, breweries) and the Web sites of alcohol distributors.

Anonymous Proxies

Includes Web sites that allow users to anonymously view Web sites.

Art / Museums

Includes Web sites from the area of theatre, museums, exhibitions, photography, graffiti, etc.

Auctions / Classified Ads

Includes Web sites with online/offline auction sites, auctions houses and online/offline advertisements.

Banking

This category contains Web sites such as banks, credit unions, credit cards and online bank accounts.

Building / Residence / Furniture

This category contains Web sites such as property markets, furniture markets, ads, equipment, design, building industry and handcraft.

Business / Services

This category includes corporate Web sites and general service providers.

Chat

This category contains Web sites that allow users to have a direct exchange of information with another user from place to place. Also listed are chat room providers and offerings about Instant Messaging.

Cinema

Includes Web sites in the area of cinema, television, program information, video-streaming, Web sites about celebrities and other entertainment sites as well.

Computer Crime

Includes Web sites containing information about the illegal manipulation of electronic devices, data networks and password encryption, as well as about credit card misuse and other methods of Internet fraud. Includes spyware and phishing sites, as well as sites providing manuals for virus and Trojan horses programming, malicious adware applications and malicious Web code.

Computer Games

Includes Web sites of computer games, computer game producers, cheat sites, online gaming zones, gaming clans and others gambling sites without chances of profit.

Dating / Relationships

This category contains Web sites that promote interpersonal relationships and escort services.

Digital Postcards

Includes Web sites that allow people to send digital postcards via the Internet, and also the providers of these services.

Education

Includes the Web sites of universities, colleges, public schools, schools, kindergartens, adult education, course offerings, history, law, dictionaries, encyclopedias and any topic hosted on universities servers.

Erotic / Sex

Includes Web sites containing nude photography and erotic material, as can be found on television or obtained free of charge from magazines. Sexually explicit activities are not listed here. Includes erotic collections of celebrities' pictures as well.

Extreme

Includes Web sites that are normally assigned to other categories, but are particularly extreme in their content (e.g. violence).

Fashion / Cosmetics / Jewelry

This category contains Web sites about of fashion (clothing, accessories), cosmetics, jewelry, perfume, modeling agencies and other Web sites of the beauty area.

Gambling

Includes lottery organizations, casinos, betting agencies, and other gambling sites with chances of profit.

General News / Newspapers / Magazines

This category contains Web sites that inform about general news, including magazines, newspapers, and magazines targeted also at younger audiences.

Governmental Organizations

Includes Web sites with content for which governmental organizations are responsible (e.g. government branches or agencies, police departments, fire departments, hospitals, military, civil defense, counterterrorism organizations) and large government organizations such as the United Nations or the European Community.

Hate and Discrimination

Includes Web sites with extreme right and left wing groups, sexism, racism, religious hate, suppression of minorities and the belittlement of National Socialism.

Health / Recreation / Nutrition

This category contains Web sites about medicine and medical care such as hospitals, doctors, drugstores, psychology, nursing, pharmaceuticals, health food stores and diet.

Humor

This category contains sites with jokes, sketches, comics and sites with other humorous content.

Illegal Activities

Includes activities that are illegal according to regional law such as instructions for murder, manuals for bomb building, instructions for illegal activity, child pornography, sodomy, instructions for cheating, etc.

Illegal Drugs

This category contains Web sites about LSD, heroin, cocaine, XTC, pot, amphetamines, hemp, stimulant drugs and the utilities for drug use (e.g. water pipes).

Illegal Software

This category contains sites with software cracks, license key lists and illegal license key generators.

Information Security

This category contains Web sites that inform people about security, privacy and data protection in the Internet and in other bandwidth services such as telecommunications.

Job Searches

Includes Web sites within the area of job offerings, job searches, job agencies, labor exchanges, temporary work, career planning, and applications for employment (CV), etc.

Music

Includes Web sites for radio, Web radio, sound files (MP3, Wav, etc.), Real Audio, homepages of singers and bands, entertainer, record labels and music vendors.

Newsgroups / Bulletin Boards

This category contains Web sites that enable the sharing of information such as on a bulletin board. Includes blogging and visitors' book servers as well.

Non-Governmental Organizations

Includes the Web sites of non-governmental organizations such as clubs, lobbies, communities, non-profit organizations and labor unions.

Online Shopping

Includes Web sites with online shops, where there is the possibility to select from a product range and order online. Includes shopping consulting, pricing and other shopping services as well.

Pharmacy / Drugs

This category contains Web sites from the pharmacy branch, as well as drugstores and information about pharmaceuticals.

Political Parties

This category contains Web sites of political parties and those sites that provide information about a particular political party and different political topics (election, democracy, etc.)

Pornography

Includes Web sites containing the depiction of sexually explicit activities and erotic content unsuitable to persons under the age of 18.

Private Homepages

This category contains Web sites about and from private individuals. Includes personal homepage servers and other sites with personal contents and activities.

Promo / Advertising

This category contains Web sites for product promotion and advertising issues with a short term durability e.g. advertisement resources received by email.

Recreational Facilities

This category contains organizations for recreational activities, for example public swimming pools, zoos, fairs and amusement parks.

Religions

Includes Web sites with religious content, information about the five main religions, and religious communities that have emerged out of these religions.

Restaurants / Bars

This category contains Web sites about bars, restaurants, discos and fast food restaurants.

Search Engines / Web Catalogues / Portals

This category contains search engines, Web catalogues and Web portals.

Shares / Stocks

Includes Web sites that handle stock exchanges rates, and deal exclusively with the main stocks like finance, brokerage and online trading. Includes Web sites about bonds, foreign currency and precious metals as well.

SMS / Ring Tones / Logos

Includes Web sites that enable a user to send short messages via SMS through the Internet to a mobile phone. It also includes providers and services for mobile phone accessories such as games, ring tones and covers.

Software and Hardware Vendors / Distributors

This category contains the complete software and hardware area. It includes the producers of hardware within the area of information, measurements and controls, as well as producers of electronic equipment. The software area includes vendors of software, freeware and shareware and software distributors. Also includes offerings concerning scripts, tolls, drivers, tutorials and other contents in the software/hardware area.

Sports

This category contains Web sites such as resort sports, fan clubs, events (e.g. Olympic Games, World Championships), sport results, clubs, teams and sporting federations, magazines and fan sites.

Swimwear / Lingerie / Nudity

Includes Web sites containing nudity, but with no sexual references. Includes illustration of swimwear and lingerie.

Tobacco

Includes Web sites dealing with tobacco and smoking (cigarettes, cigars, pipes), and Web sites from tobacco vendors.

Translation

This category contains Web sites that enable the translation of parts or the entire content of a Web site into another language. Dictionaries and 'language' topics are not listed here.

Travel

Includes Web sites about destinations, monuments, buildings, sights, travel agencies, hotels, resorts, motels, airlines, trains, car rental agencies and general tourist and travel information.

Unclassified

This category is the default category for any site that is pending classification.

Weapons

This category deals with firearms and accessory, weapons such as knives, ammunition and tear gas, other weapons and Web sites of military/paintball topics.

Web Hosting / Bandwidth Services

Includes offerings and services for publication of Internet sites (such as Web hosting, Web design, advertising and marketing companies), domain registration and Internet Service Providers as well as providers of broadband services and others related topics.

Web Mail

This category contains Web sites that enable Internet users to send or receive emails through the Internet (mailbox). All providers of Web mail services are categorized here as well.

KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted email messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today, Kaspersky Lab employs more than 1000 professionals. Nine of them hold M.B.A. degrees and fifteen hold Ph.Ds. The leading analysts at Kaspersky Lab are members of the Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company's specialists to foresee trends in the development of malware and to provide our users with timely protection against new types of attacks. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks including workstations, file servers, mail systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools maximize the degree of automation of anti-virus protection of computers and corporate networks. Many well-known manufacturers use the Kaspersky Anti-Virus kernel in their products, including: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. We plan, install, and support corporate anti-virus suites. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. Detailed consultations are provided by phone or email. You will receive full answers to all of your questions.

Kaspersky Lab official site:	http://www.kaspersky.com
Virus Encyclopedia:	http://www.viruslist.com
Anti-virus laboratory:	newvirus@kaspersky.com (only for sending suspicious objects in archives) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en (for virus analysts queries)